UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería de Tecnologías y Servicios de la Telecomunicación.

TRABAJO FIN DE GRADO

Estudio de ciberataques mediante el análisis de tráfico en Internet.

Eric Crusi Mozota

Tutor: Luis de Pedro Sánchez

Ponente: Jorge Enrique López de Vergara

Junio 2018

Estudio de ciberataques mediante el análisis de tráfico en Internet.

AUTOR: Eric Crusi Mozota

TUTOR: Luis de Pedro Sánchez

Computación y redes de alta prestaciones

Dpto. Tecnología Electrónica y de las Comunicaciones

Escuela Politécnica Superior

Universidad Autónoma de Madrid

Junio de 2018

Resumen (castellano)

En los últimos años el tráfico en Internet ha aumentado exponencialmente y con esto también los ataques en la red. Además, cada vez estos ataques se hacen más difíciles de detectar por los sistemas que se encargan de la ciberseguridad. Por tanto, la necesidad de tener más métodos para protegernos frente a estos ataques es de vital importancia y por ello hay que entender la forma que tienen y cómo afectan a las características del tráfico.

Junto con el aumento del tráfico y de los ataques, también se han desarrollado varios modelos estadísticos y sistemas que tienen como meta analizar este tipo de tráfico y ver las características que éste tiene para así proporcionar información sobre cómo actuar frente a dichos ataques.

El objetivo de este trabajo consiste en usar uno de los modelos que mejor se adapta a la hora de analizar el comportamiento de la red y extraer información acerca de esta. El modelo que vamos a usar se le denomina Alfa estable y con él vamos a analizar un conjunto de datos que están disponibles en la red por parte de la universidad de Granada.

El conjunto de datos que proporciona está formado por flujos extraídos de una red real y por varios flujos de tráfico sintético de ataque. El análisis consiste en ver cómo responde este el modelo frente al tráfico real, al tráfico sintético y a la mezcla de estos dos, de esta manera generaremos un tráfico que represente un ataque en una red real.

Palabras clave (castellano)

Flujos, Matlab, Alfa estable, anómalo, AWK, denegación de servicio, modelo estadístico, distribución de probabilidad, Shell script, netflow.

Abstract (English)

In the last few years, Internet traffic has increased exponentially and consequently network attacks have soared too. In addition, these attacks are becoming increasingly difficult for systems to detect by the cybersecurity systems. Therefore, the need for more methods to protect ourselves from these attacks is of vital importance and we must therefore understand how they affect traffic and how they affect it.

Along with the increase in traffic and attacks, there also has been an increase in the various statistical models and systems that aim to analyze this type of traffic and see the characteristics that they have in order to provide information on how to act against them.

The aim of this work is to use one of the models that best fits when analyzing the behavior of the network and extract information about it. The model we are going to use is known as Alfa stable distribution and with it; we are going to analyze a set of data that are available on the Internet from the University of Granada.

The set of data it provides consists of flows extracted from a real network and several flows of synthetic attack traffic. The analysis consists of seeing how the model responds to real traffic, synthetic traffic and the mixture of both, with we will generate traffic that represents an attack on a real network.

Keywords (English)

Flows, Matlab, Stable alpha, anomalous, AWK, denial of service, statistical model, probability distribution, Shell script, netflow.

Agradecimientos

Antes de empezar con el trabajo me gustaría agradecer a la cátedra UAM Naudit y a la Universidad de Granada por proporcionarnos los datos necesarios para realizar este trabajo.

También agradecer a mis tutores por toda la ayuda que me han dado, incluyendo los miles de emails que hemos mandado y las conferencias por Skype. A mi familia por todo el apoyo que me ha dado en los momentos de estrés, a mis compañeros de carrera la ayuda que me han dado a lo largo de los años, en especial a Jorge Benedicto y Alejandro Peña, y a mis amigos de fuera de la carrera por aguantarme durante este periodo, en especial a Guillermo Fernández y Daniel Blázquez.

INDICE DE CONTENIDOS

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

Glosario

IP	Internet Protocol
PDF	Función Probabilidad de Densidad

1 Introducción

En este capítulo se exponen los hechos por los cuales se ha llevado a cabo este Trabajo Fin de Grado, los objetivos que tiene y cómo está estructurada la presente memoria.

1.1 Motivación

El estudio de las herramientas para detectar anomalías en la red es un campo de gran interés debido al aumento de ataques que se han producido en las últimas décadas. Además, estos ataques cada vez estos ataques se hacen más difíciles de detectar. Un ejemplo inmediato de esto es el caso que se verá a continuación en el trabajo, en el cual cuando comparamos el flujo de datos que no ha sufrido anomalías con el que sí las ha sufrido y observamos los bits por segundo de la conexión, no se aprecia ninguna diferencia entre ellos. Sin embargo, esto no significa que el ataque no se pueda detectar, sino que el análisis que estamos analizando de los flujos es inútil.

Por otra parte, el análisis de tráfico a través de flujos temporales facilita mucho la tarea de ver cómo estos se comportan. Los flujos de datos se pueden extraer de Internet con herramientas como netflow, la cual se ha usado para extraer los datos. Con esta herramienta el manejo de datos es mucho más cómodo puesto que nos facilita las características del flujo necesarias para proceder con el análisis.

El trabajo consistirá en analizar los datos de estos flujos y ver cómo se comportan estos frente a cambios en sus datos a través del modelo Alfa-estable.

1.2 Objetivos

El objetivo principal de este TFG consiste en el estudio de análisis de flujos de datos temporales de tráfico que ha sufrido algún tipo de anomalías y ver qué características se ven modificadas. Para ello se ha seguido un proceso con el fin de ver las conclusiones del estudio realizado. Este proceso se divide en:

- Extraer los datos de los archivos.
- Calcular sus bits y paquetes por segundo con la herramienta AWK.
- Calcular los parámetros alfa estable de los bits o paquetes por segundo en las zonas donde se producen las anomalías con la herramienta Matlab.
- Representar dichos valores y analizar las diferencias entre ellos.

1.3 Fases de realización

En este apartado expondremos a modo de resumen las fases que se han ido realizando hasta llegar al resultado final de este trabajo de fin de grado. Dichas fases son:

- **Estudio de alfa estables:** Se ha realizado un estudio acerca del modelo de los parámetros alfa estable saber que representa cada uno de ellos. Además del estudio de estos valores también se ha investigado acerca de cómo interactúan estos con el tráfico en internet. Se tendrá en cuenta que las variables aleatorias que pondremos en el modelo serán los bits y los paquetes por segundo.

- **Extracción de la primera serie de datos:** Una vez se ha entendido el comportamiento de los valores alfa estable, pasamos a extraer y analizar el conjunto de datos proporcionados por la Universidad Autónoma de Madrid. Estos datos vinieron dados en dos formatos, los flujos de datos de cada día durante esas semanas y la semana completa. Se calculó los bits por segundo de ambos formatos y a la hora de comparar los datos de flujo de un día, con el de la semana ya compuesta, encontramos que la suma de sus bytes totales tenía un error de 10%, por lo que se decidió desestimar estos datos.

- **Funciones de Matlab:** Se estudiaron las funciones que utilizan este tipo de variables aleatorias y cuáles eran las más útiles para realizar el análisis de los datos.

- **Extracción de la segunda serie de datos:** Se encontró un nuevo conjunto de datos proporcionado en un servidor por parte de la Universidad de Granada. Este nuevo conjunto de datos aparte de los flujos del tráfico sondeado también subió tráfico sintético de varios tipos de ataque.

- **Cálculo de los parámetros alfa estables y representaciones:** Con los datos ya extraídos y analizados, creamos ventanas de varios tamaños temporales para calcular los valores de alfa estable en todas las zonas de especial interés.

- **Análisis:** Observamos las representaciones y se observaron cómo los valores que presentaban los valores de alfa, beta, gamma y delta. La variación de estos parámetros dio lugar a conclusiones que se presentarán a lo largo del trabajo.

A continuación, se presenta el diagrama de Gantt correspondiente al trabajo realizado:

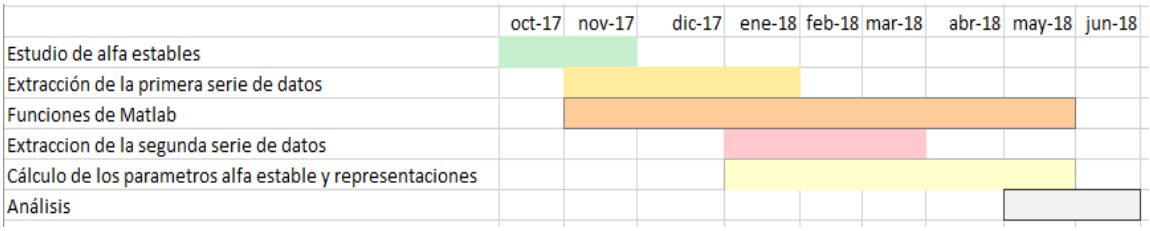


Ilustración 1.1 Diagrama de Gantt.

1.4 Organización de la memoria

La memoria consta de los siguientes capítulos:

- **Capítulo 2: estado del arte**: donde se explicarán los conceptos necesarios para entender todos los conceptos necesarios de cara a este trabajo.
- **Capítulo 3: diseño y desarrollo**: en esta sección se mostrará y desarrollará como se ha planteado el trabajo y las varias decisiones que se han tomado.
- **Capítulo 4: pruebas y resultados:** se comentarán cómo se han realizado las pruebas junto con las variaciones de estas.
- **Capítulo 5: conclusiones y trabajo futuro:** con los resultados obtenidos en el capítulo anterior se comentarán los hechos por los cuales se dan estas características y los posibles trabajos que se podrán realizar a partir de estas conclusiones.

2 Estado del arte

2.1 Introducción

En esta sección vamos a presentar y desarrollar los conceptos más importantes que están relacionados con este trabajo de fin de grado, para así tener un mayor entendimiento y dominio de estos.

2.2 Ataques de red

Un ataque de red [1] es un intento de acceder a un sistema informático a distancia, en el cuál el que realiza la conexión intenta quedarse al mando del sistema al que se conecta, deniega el servicio o consigue información confidencial.

Existen varios tipos de ataques [2] como los de actividades de reconocimiento de sistemas, detección de vulnerabilidades en los sistemas, robo de información mediante la interceptación de mensajes, modificación del contenido y secuencia de los mensajes transmitidos, análisis de tráfico, ataques de suplantación de la identidad y de denegación de servicio. Este último será el caso principal de estudio.

El ataque de denegación de servicio (DoS) [3] tienen como objetivo provocar que un servicio o recurso no esté disponible, haciéndolo inaccesible, para el usuario que tiene derecho a usarlo. Esto puede hacer que una maquina deje de dar servicios a todo el mundo, que solo de algunos o que solo de servicio a un determinado grupo de personas.

Aparte, también existe la Denegación de Servicio Distribuido (DdoS) [3], funciona igual que denegación de servicio, pero se usan múltiples ordenadores para realizar un ataque coordinado a una misma máquina. En el proceso de este tipo de ataque, se usan unas máquinas que se denominan Zombies, las cuales las consigue la persona que ataca y las controla a través de un programa que ha introducido.

2.3 Flujos de red (NetFlows)

Un flujo de red o NetFlows [4] es herramienta de análisis de flujos que llegan en orden y comparten protocolo, direcciones IP y puertos de origen y destino. Los datos, además de estos campos, presenta muchos más que pueden ser útiles también para el análisis. Las características de la tecnología de NetFlow nos permite realizar todo tipo de tareas tales como:

- La monitorización.
- La predicción de ataques.
- La detección de intrusos.

En este trabajo nos vamos a centrar en el análisis de estos flujos para determinar si se producen ataques en la red.

Además, gracias a las estadísticas que ofrece, como los tiempos de inicio y fin de flujo, el tamaño en bytes, el número de paquetes se va a poder realizar un análisis sobre una serie de flujos utilizando herramientas adicionales.

Hay que tener en cuenta que un flujo, suele considerarse acabado cuando no se observa ningún tipo de tráfico durante 15 segundos, cuando recibe el flag de fin de conexión o si está activado desde hace 30 minutos.

2.4 Distribución alfa estable

Las distribuciones estables [6] son una clase de distribuciones de probabilidad en las que se permiten las asimetrías y las colas pesadas, además de tener propiedades matemáticas interesantes para el análisis de tráfico.

Una propiedad importante que haremos uso en este trabajo, es que la suma de dos variables aleatorias es una variable aleatoria. Partiendo de esto podemos asumir [7] que una variable aleatoria X sigue una distribución alfa- estable si para dos números positivos A y B, existe un número C y otro real D tal que se cumple:

$$A\boldsymbol{X_1} + B\boldsymbol{X_2} \stackrel{d}{=} C\boldsymbol{X} + D$$

Siendo X1 y X2 dos copias independientes de X. Esto demuestra que la suma de dos variables alfa-estable sigue siendo alfa-estable.

Una definición adicional sería: se dice que una variable aleatoria X es alfa-estable si existen parámetros en los que $\alpha \in (0.,2]$, $\beta \in [-1.1]$, $\gamma \geq 0$ y $\mu \in \mathbb{R}$ y en los que X tiene la forma de:

$$E\{\exp(it\boldsymbol{X})\} = \begin{cases} \exp\left\{-\sigma^{\alpha}|t|^{\alpha}\left[1 - i\beta \mathrm{tg}\left(\frac{\pi\alpha}{2}\right)\mathrm{sgn}(t)\right] + i\mu t\right\} & \alpha \neq 1 \\ \exp\left\{-\sigma|t|\left[1 + i\frac{2\beta}{\pi}\mathrm{sgn}(t)\log(|t|)\right] + i\mu t\right\} & \alpha = 1 \end{cases} \quad \text{(A.3)}$$

[7]

Los parámetros alfa estable presentan las siguientes características:

- Alfa, α, define la estabilidad de la función o el equivalente que veremos en el trabajo la forma de la curva. Es el valor más representativo.
- Beta, β, determina la simetría de la función.
- Gamma, γ, se usa para definir la escala de la distribución.
- Delta, δ, representa la localización relativa de la función.

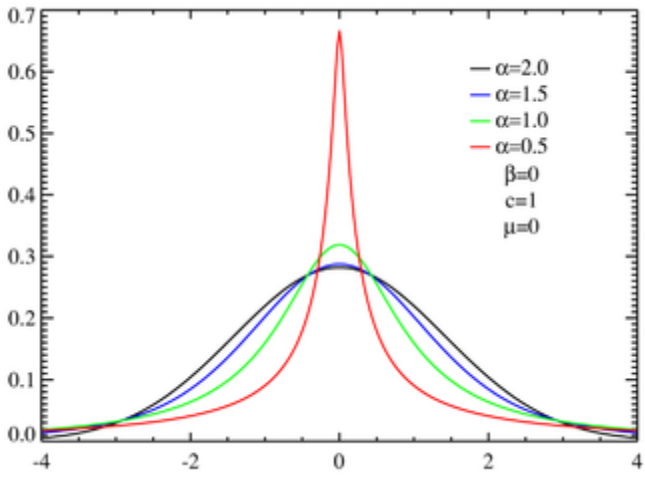


Ilustración 2.1 Distribución alfa-estable [8]

2.5 Conclusiones

Como resumen del capítulo, podríamos decir que los flujos de red son los que contienen la información necesaria para que podamos realizar el análisis del tráfico de una red IP. Dentro de esos de esos flujos puede haber algún determinado tipo de ataque y en este trabajo lo que se quiere es estudiar sus diferencias con respecto a un tráfico que no haya sido afectado por ninguna intrusión. La distribución alfa estable como modelo estadístico es parte de las herramientas que se van emplear en el estudio.

3 Diseño y desarrollo

3.1 Introducción

En este capítulo se muestra el proceso que se ha seguido en este trabajo. Además, en cada sección se explicará el motivo por los cuales se han tomado tales medidas y más adelante se exponen las repercusiones que tienen.

3.2 Generación de series temporales

Lo primero que hubo que hacer fue extraer las series temporales y ver como estaban organizadas para poder trabajar con ellas. El formato de extracción fue realizado con la herramienta de Linux, nfdump [2], el cual descomprime los archivos de red en un archivo .csv formado por los siguientes campos: el tiempo de finalización del flujo, la duración del flujo, la dirección IP de origen, el destino, el puerto de origen y destino, el protocolo que se usa, los flags, el tipo de servicio, el número de paquetes que ha habido en ese flujo y el número de bytes.

Los campos que decidimos guardar en el fichero .csv con el que trabajamos fueron, *tiempo de finalización del flujo*, *duración del flujo*, *bits y paquetes* que se han transmitido por el flujo. Además, se vio la necesidad de realizar el cálculo del tiempo de inicio de un flujo para poder realizar el esquema que se verá a continuación.

Una vez estructurados los campos del .csv empezamos con la primera decisión que se tomó a la hora de obtener los datos característicos del flujo, la cual fue suponer que el comportamiento de los flujos era uniforme en toda su duración. Esta decisión se realizó para poder medir el tanto el número de bytes y de paquetes que había en cada segundo en cada uno de los flujos de una manera más sencilla para facilitar la labor del trabajo. Con esto nos encontramos con un nuevo problema, el cual fue cómo repartir estos valores en cada segundo. Para solucionar este problema se propuso el modelo que se va a ver a continuación, en la **¡Error! No se encuentra el origen de la referencia.** se puede observar el modelo. Se representa cada flujo esquemáticamente como un segmento cuyos extremos son los instantes de inicio y fin del flujo, datos extraídos del fichero .csv:

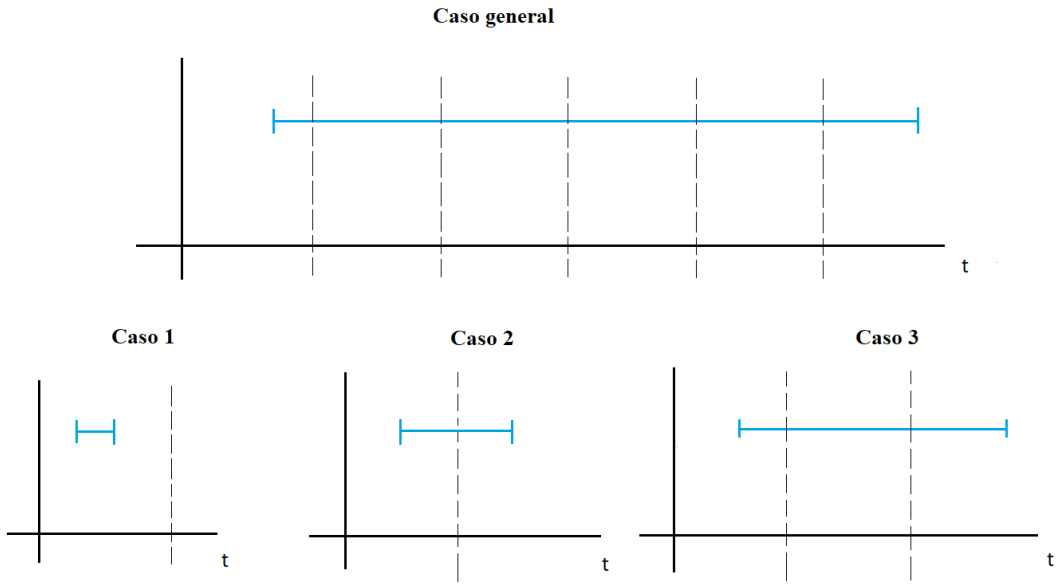


Ilustración 3.1 Esquema de tratamiento de flujos.

El procedimiento a seguir para estimar la serie temporal correspondiente a un flujo se puede dividir en tres casos partiendo del caso genérico. Antes de seguir con la explicación del proceso es importante aclarar que significa cada línea. Las líneas azules representan los flujos y su duración. Las líneas verticales discontinuas representan el inicio y el fin de una unidad de tiempo (segundo). Y, por último, los ejes representan el array sobre el que se ha ido calculando el número de bits/paquetes por segundo.

La serie temporal se analizará con una resolución de un segundo y suponiendo que los flujos son uniformes a lo largo de toda su duración. Esto lleva a que el tratamiento de los diferentes casos sea distinto.

En el caso 1 se observa que la duración del flujo se sitúa entre el principio y el primer segundo. Este caso se vio necesario puesto que cuando se empezó a analizar los datos, los paquetes que tenían duración menor a un segundo no se tenían en cuenta lo que hacía que la representación de la serie temporal fuera muy incorrecta, aunque esto se comentará más adelante. En este caso los bytes o paquetes como no llegan al segundo entero se asigna al segundo más cercano redondeando hacia abajo. En el caso 2 el flujo se sitúa en mitad de un segundo, en este caso el flujo se asocia de manera parecida al caso 1, la parte correspondiente de la izquierda se asigna al segundo entero mientras que el siguiente se asigna al segundo

donde ha cortado, es decir, si la discontinua fuera el valor 1 segundo y la duración de 1 también y están repartidas en la misma medida, los bytes/paquetes se reparten por igual en ambos lados. El lado de la izquierda asigna al segundo 0 la mitad de ese flujo y el segundo 1 asigna la otra mitad. Por último, el caso 3 es una representación más simple que del caso genérico donde la repartición de los valores se podría decir que es una mezcla de los casos 1 y 2 comentados anteriormente, de manera que cuando se trate del caso genérico lo que se hace es recorrer la duración de cada flujo con intervalos de un segundo entre ellos para ver cuanta carga de flujo hay en ese punto.

De esta manera, los cálculos para representar la serie temporal ya estarían realizados y su representación sería la siguiente:

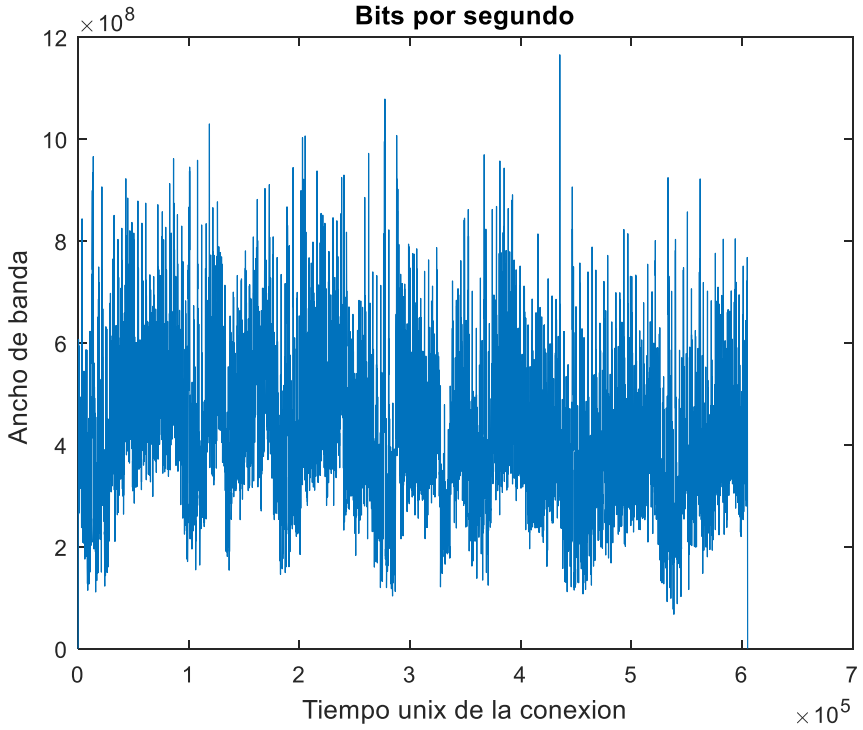


Ilustración 3.2 Bits por segundo.

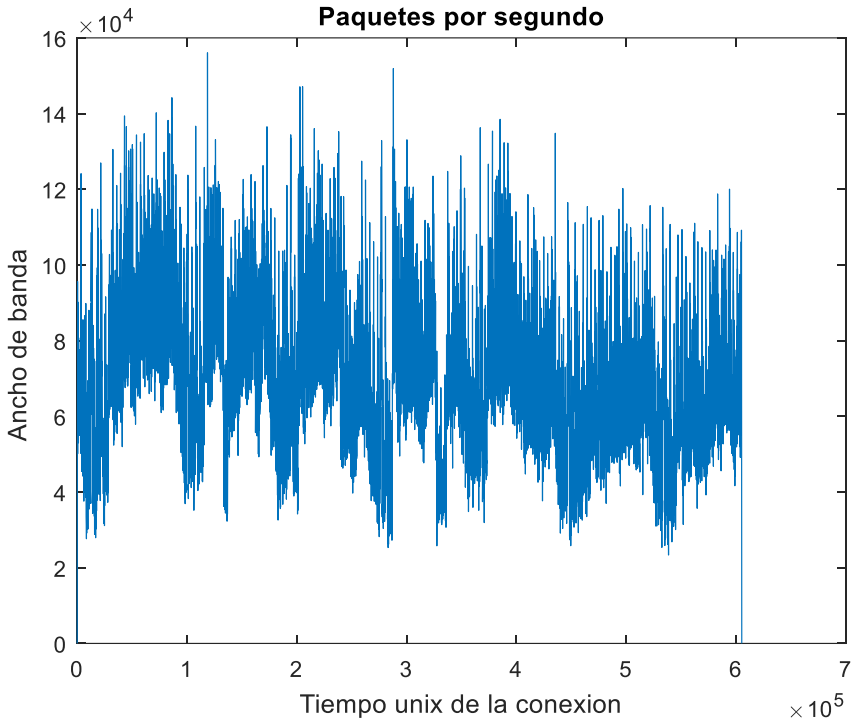


Ilustración 3.3 Paquetes por segundo.

3.3 Estimación de parámetros estadísticos

El motivo por el cual se ha elegido obtener los distintos valores estadísticos como la media, moda, mediana, desviación típica, varianza, los valores de los parámetros alfa-estable o el algoritmo para obtener los parámetros necesarios de los archivos vienen reflejados junto con los programas usados viene explicados en esta sección.

Un esquema del proceso seguido se puede ver en la Ilustración 3.4. Como se ha mencionado en el apartado anterior, hubo que extraer los datos de las series temporales y ver con que columna nos resultaba útil, Esta extracción se tuvo que hacer siguiendo un determinado orden, para que los datos como los tiempos de llegada y tamaños de byte o número de paquetes no se vieran alterados. Hubo que hacer varias conversiones de datos a formatos con los cuales se pudieran operar de manera más cómoda para así finalmente, como se explicará más adelante, calcular el número de bytes por segundo o paquetes por segundo y tener el resultado que queríamos. Esta parte se realizó con un programa escrito en AWK debido a que ofrecía menor tiempo y menor complejidad que cualquier otro a la hora de calcular línea a línea las series temporales.

Después de obtener los datos necesarios, estos, se pasaron a la plataforma de Matlab para obtener representaciones de dichos valores y poder operar con filas y columnas con mayor facilidad. Además, este programa nos permitió calcular los valores estadísticos que se han mencionado al principio. Sin embargo, no solo se escogió esta plataforma por esos motivos, si no que añadiendo una librería extra nos daba la posibilidad de calcular los valores que determinaran el resultado de este trabajo, los parámetros alfa-estable. La librería usada se denomina STBL. Para la obtención de estos valores se usó una ventana deslizante con el fin de ver como variaban en cada segundo dichos parámetros. El tamaño de la ventana ideal es de 900 puntos, puesto que a la hora de obtener los histogramas que se verán más adelante se necesita que tengan un buen rango de valores. Sin embargo, este valor a lo largo del trabajo va a variar puesto que la ventana se tiene que poder adaptar a cada zona de interés. Además, nos interesa que la ventana pueda empezar desde cualquier punto de las series temporales y no tener que esperar a que llegue a dicha zona, por lo tanto, para la creación de dicha ventana pasamos varios argumentos que indican las características de esta.

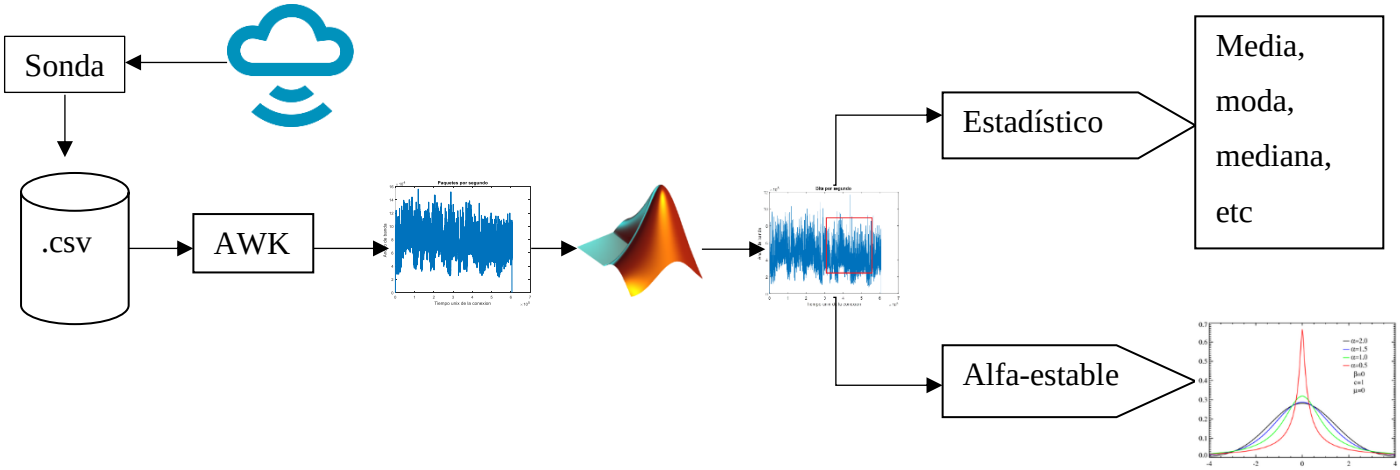


Ilustración 3.4 Esquema del proceso de datos.

3.4 Datos analizados

Los datos que se han usado a lo largo de la realización de este trabajo se han adquirido de dos fuentes distintas. La primera serie de datos fue facilitada por la cátedra UAM Naudit y la segunda serie de datos se descargaron de una base de datos que la Universidad de Granada usó para otras pruebas [5].

La principal diferencia de estas series de datos es que la segunda serie, además de proporcionar series temporales extraídas de un entorno real, presentaba archivos creados de manera sintética que alteraban el tráfico real y con los cuales se ha llevado a cabo el trabajo.

- La primera serie de datos vino con dos formatos distintos, un primer formato el cual estaba formado por varios archivos de texto que correspondían a los días de las dos semanas y el segundo formato eran dos archivos de texto los cuales correspondían cada uno a la primera y a la segunda semana de ese mismo análisis.
- La segunda serie de datos a diferencia de la primera contenía archivos los cuales ya eran una semana de análisis. La base de datos de esta segunda serie incluía varios meses, pero solo escogimos una semana como análisis. Además de presentar solo un archivo respecto a la semana, se adjuntaron a la semana correspondiente los archivos creados de manera sintética mencionados anteriormente junto con una tabla sobre cuando se aplicaron los ataques a las series reales.

La necesidad de buscar una segunda serie de datos se vio cuando al analizar la primera serie y obtener su representación de bytes por segundo a lo largo de la semana formada por días y compararla con el archivo de la semana correspondiente se observó que no presentaban la misma forma, además la suma acumulada de los bytes a lo largo de la semana comparada con su correspondiente semana presentaba un error del 10% por lo que se decidió descartar dicha serie de datos. Además de este factor decisivo, también se encontraron otros problemas como no saber cuándo acababa y cuándo empezaba la sonda en la extracción de datos en la red.

3.5 Programas desarrollados

En este apartado vamos a explicar cómo funcionan los algoritmos aplicados de cada uno de los programas que se observar en la ilustración anterior.

El primer programa que se usó fue el de AWK, el cual más adelante se le añadió una funcionalidad más que explicaremos a continuación. El comportamiento de este programa viene dado por los siguientes pasos:

- El documento original de la serie de datos venía con unos caracteres que hubo que cambiar para poder cambiar el formato de la fecha de fin del flujo y poder calcular el tiempo de AA-MM-DD HH: MM: SS a tiempo Unix en UTC.

- Una vez con la fecha cambiada a un formato que permite operar con mayor facilidad se realizaron el resto de cálculos de los campos necesarios para obtener la representación de los datos respecto del tiempo. El tiempo de inicio del flujo se calculó restando la duración del flujo a la fecha a la que anteriormente cambiamos su formato. Además, se tuvo que sumar las dos horas de diferencia con la que venía el formato Unix en UTC. A su vez los bytes se pasaron a bits y se guardaron los otros campos en el archivo de texto que usaremos para el siguiente paso.
- Una vez se tenían los datos calculados, ante cualquier posible error a la hora de guardar los valores originales, se ordenaron de menor a mayor respecto al tiempo de inicio del flujo. Además, se observó que tras este ordenado había que borrar la primera línea del archivo resultado puesto que esa línea no tenía campos leíbles.
- Después de este proceso, se ya procedió al cálculo de los bits y paquetes por segundo siguiendo un determinado algoritmo. Este algoritmo consistía en usar las partes enteras de la fecha para indexar esos valores en un array, tal y como se explicó en la ilustración 3.1. Este array se iba llenando de varias maneras dependiendo del caso en el que se encontraba el flujo, del tamaño; los bits/paquetes se calculaban de distintas formas.
- La funcionalidad que se le añadió fue mezclar el tráfico sintético de ataque con el tráfico real extraído. Este procedimiento se realizó juntando ambos tráficos y ordenarlos con el mismo criterio que se hizo anteriormente.

El segundo programa se desarrolló en Matlab, para recibir los datos resultantes del primer programa. En este programa se realizaron dos cosas distintas una sin la librería y otra con la librería STBL por lo que la explicación se dividirá en dos secciones. En la primera parte se realizó lo siguiente:

- Primero se leyeron los archivos originales, los que pasaron por el proceso de mezclado y los de ataque sintéticos y se representaron para ver la forma que presentaban, esto se verá en el capítulo 4.
- Se guardaron en una variable los valores donde en el tráfico sintético de ataque presenta sus máximos puesto que estos valores son los que afectaran al tráfico. Se buscó cuándo se producían estos picos en el archivo sintético y acto seguido, dónde se producían estos en el archivo mezclado para saber en qué posición respecto al original es la que ha sufrido el ataque. Esto se debe a, que como veremos en el

siguiente capítulo, no presentan diferencias entre ellos. La búsqueda se realizó en el archivo mezclado como podría haberse realizado en el archivo original puesto que ambos comparten el mismo eje de tiempos.

- Una vez se tiene localizado el ataque, se realizó el estudio estadístico con los valores más comunes para ver si se producía alguna diferencia. Este estudio se vio determinado por una ventana a la cual se le indicaba donde empezaba y donde acababa junto con el tamaño de esta, puesto que no es lo mismo realizar la media en 15 minutos justo cuando se produce el ataque que realizarla en esos mismos 15 minutos, pero 7 antes y 8 después del punto en el que se produce el ataque. La longitud de la ventana viene dada en segundos. En el caso que se va a mostrar en las ilustraciones siguientes el análisis empieza justo en el ataque y 15 minutos después. Sin embargo, la ilustración 3.5 muestra un ejemplo de la ventana sin tener en cuenta los tiempos. El punto en el que empieza el recuadro es el instante inicial y su longitud equivale al tamaño de la ventana en segundos.

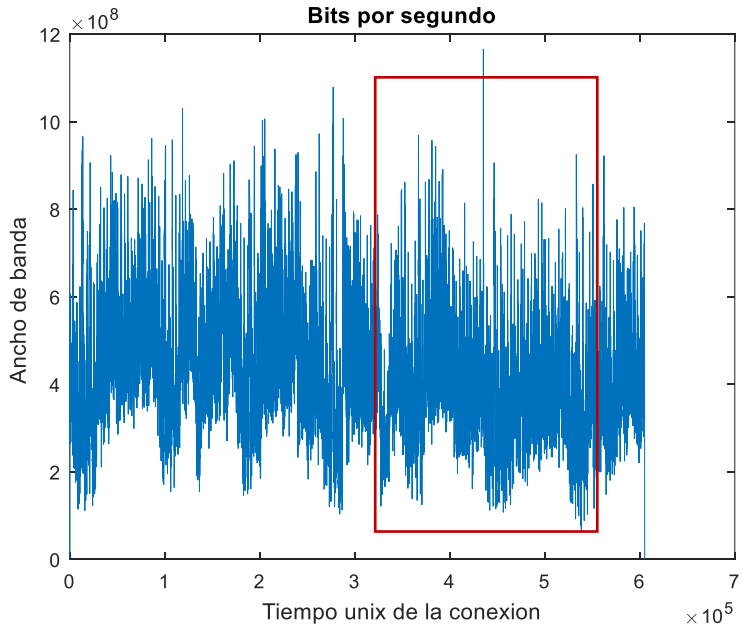


Ilustración 3.5 Ejemplo de la ventana deslizante.

- Y por último se calcularon las funciones de probabilidad de densidad de cada uno de los datos en las zonas de interés.

En la segunda parte destaca el uso de la librería donde se calcularon los valores del modelo alfa-estable. Se crearon dos funciones que usan completamente esta librería, una llama a la otra puesto que una realiza todo el cálculo y la otra se encarga de variar donde se produce el

cálculo. Para aclarar en la explicación de a continuación llamaremos a la función que se encarga del cálculo, parametrización y a la segunda función cálculo del array de alfas.

- A la primera función le llegan varios valores, pero nos centraremos en los más importantes. Estos son los datos de los que se quiere calcular los parámetros, la duración de la ventana fija, el punto donde empezará dicho cálculo y el tipo de dato ya sean bits o paquetes.
- Se llama a continuación a la función propia de la librería llamada stblfit a la cual le pasamos los datos desde el punto inicial y hasta el tamaño de la ventana. Esta función de vuelve los valores en un array y los extraemos en otros valores para más adelante pasar estos en otra función llamada stblpdf. Esta función simula la función de probabilidad de densidad con los valores que le pasamos de alfa, beta, gamma y delta. La función parametrización devuelve los valores de alfa, beta, gamma y delta.
- Comparamos las gráficas que devuelve la función y la de los histogramas para ver el comportamiento que tiene.
- La segunda función se encarga de llamar a parametrización, pero con una serie de cambios. A parte de los mismos valores de la primera función, ésta recibe valores para indicar desde donde empieza el análisis y donde acaba, de manera que se puede indicar el tiempo donde empieza el ataque, la duración de la ventana y dos separaciones, que explicaremos su motivo a continuación. Esta función devuelve un array de los valores del modelo alfa-estable que van variando respecto del tiempo.
- Los valores de separación se encargan de indicar la distancia en la que empieza respecto al valor de inicio y donde acaba después, teniendo en cuenta después que la ventana fija de la primera función no sobrepase la deslizante que se está formando en este caso.

3.6 Conclusiones

En este capítulo se observan y explican todos los procesos que han sido necesarios a la hora de realizar el trabajo. Además, se explica el motivo por el cual se han elegido los programas y de que se encarga cada uno de manera más específica. La librería usada presenta una gran utilidad en el análisis puesto que, sin ella, habría que haber buscado otra manera igual de eficaz de calcular los parámetros alfa-estable.

A continuación, en el capítulo 4 se observarán la representación de las series de datos reales, mezclados y sintéticos y las diferentes pruebas de ventanas realizadas sobre estos y como el alfa-estable destaca por encima de los valores estadísticos más usados

4 Pruebas y resultados

4.1 Introducción

En este capítulo se explica la metodología usada para el análisis de los datos obtenidos junto con los resultados. Además, se mostrarán los distintos tipos de ataques que hemos realizado y ver la diferencia entre ellos y como estos modifican o no los parámetros.

4.2 Metodología

En esta sección vamos a exponer los valores que se han usado para el proceso de análisis que se ha explicado en el capítulo 3. Hay que aclarar que, a la hora de mezclar el tráfico normal con los distintos tipos de ataque, el estadístico podría verse alterado con solo introducir otra serie de datos. Sin embargo, como el tráfico real es mezclado con un tráfico cuyo tamaño en comparación es menor del 1% no hay motivos por los que suponer de que esto suceda, haciendo que el análisis que estamos realizando sea consistente.

Por otra parte, el análisis se ha realizado con varias medidas de tiempo y tamaños de ventana distintos. Las ventanas usadas para la extracción de parámetros alfa-estable han sido de 2 minutos, y de 15 minutos junto con las estadísticas de media, moda, mediana, varianza y desviación típica. Además, dentro de esos 15 minutos se han analizado los datos en un tramo de dos horas antes y dos horas después para ver si el ataque en ese periodo es perceptible o no, siendo la variable aleatoria los bits o los paquetes por segundo. El único uso de los 15 minutos en el tramo de las dos horas se debe a que con este número llegamos a lo que se comentaba anteriormente del tamaño ideal de la ventana que son 900 puntos, esto es debido a que obtendremos una mayor resolución de datos en los histogramas, puesto que la medida de tiempo corresponde a un punto un segundo.

En el siguiente apartado veremos dos tipos de ataque y las diferentes gráficas que se han obtenido para ver qué ocurre en los casos propuestos.

4.3 Tipos de ataque

4.3.1 Denegación de servicio

Uno de los ataques que hemos realizado es el de denegación de servicio. Aunque se haya explicado en que consiste el ataque, el caso práctico se basa en lo explicado en el capítulo 3 respecto a la creación de las series. En este caso el tiempo de ataque en concreto que vamos a analizar tiene una duración de 2 minutos por tanto se representaran las gráficas centradas en el tiempo que se ha producido el ataque tal y como se ha explicado antes. Como se puede observar por inspección, es imposible diferenciar a simple vista el tráfico normal del tráfico con ataque

Primero expondremos los bits por segundo del tráfico normal, el mezclado y el sintético de ataque de manera que se observe la forma que tiene y acto seguido se enseñaran las gráficas de los diversos tamaños elegidos de ventana. Aunque ya se haya mostrado el tráfico normal anteriormente, es importante volverlo a mostrar para ver que no se percibe diferencia.

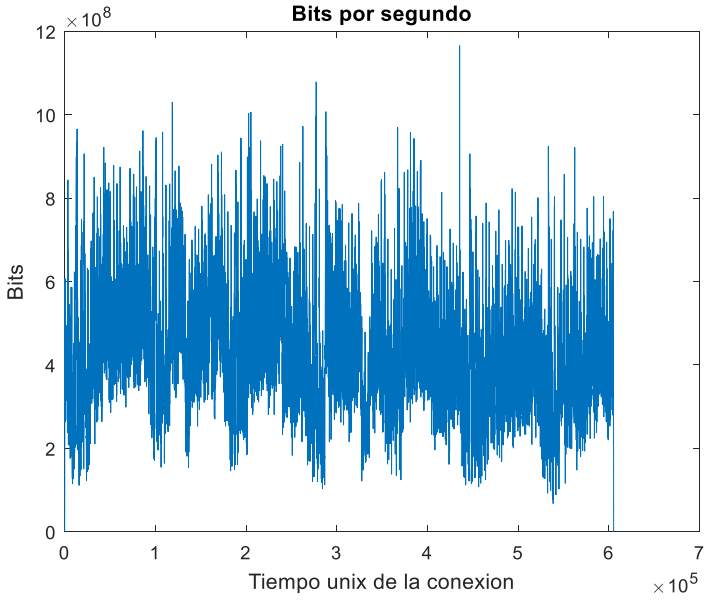


Ilustración 4.1 Bits por segundo.

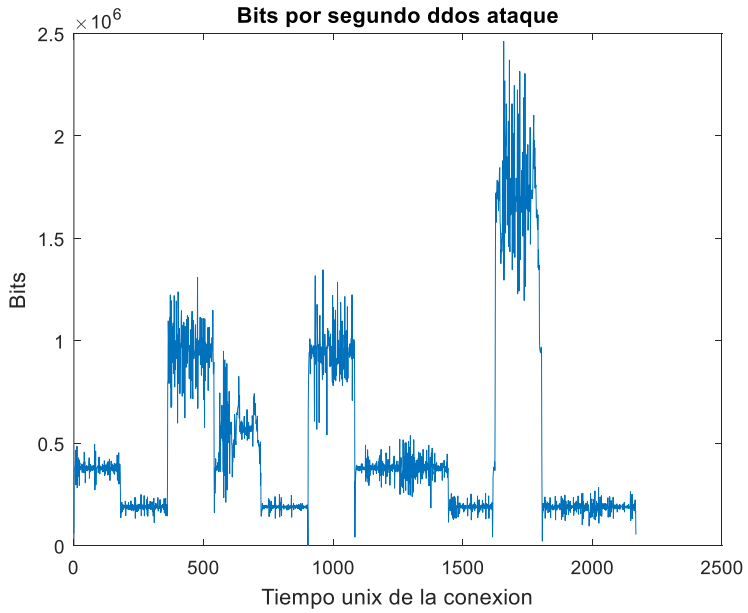


Ilustración 4.2 Tráfico sintético de ataque en bits

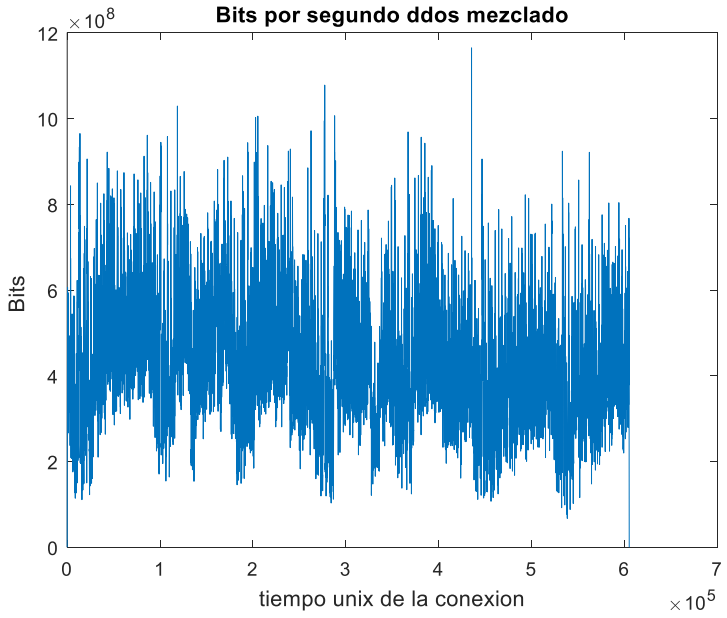


Ilustración 4.3 Tráfico mezclado en bits.

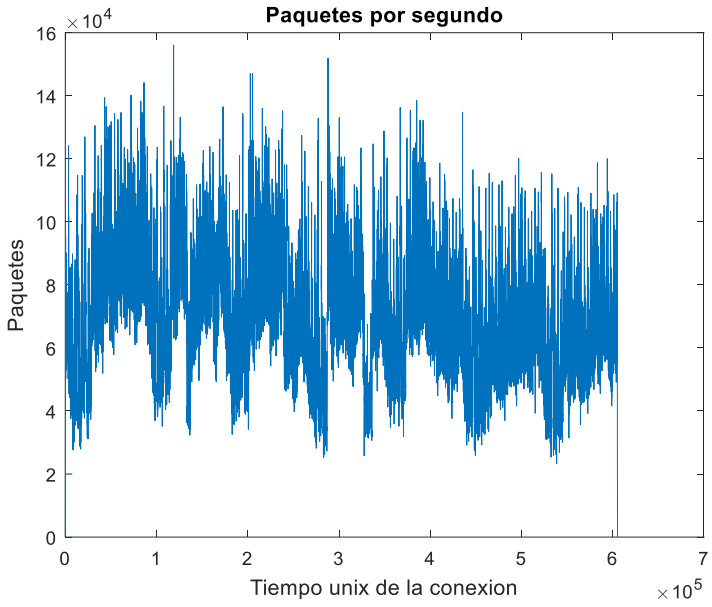


Ilustración 4.4 Tráfico real en paquetes.

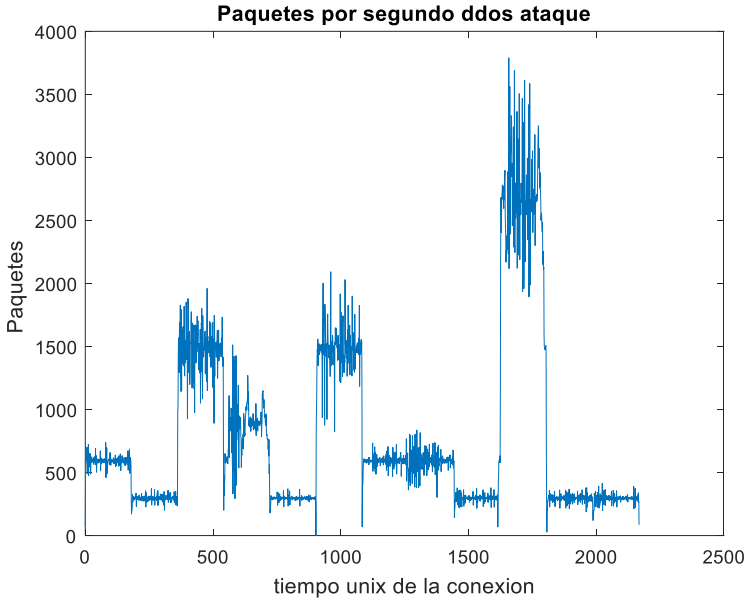


Ilustración 4.5 Tráfico de ataque en paquetes.

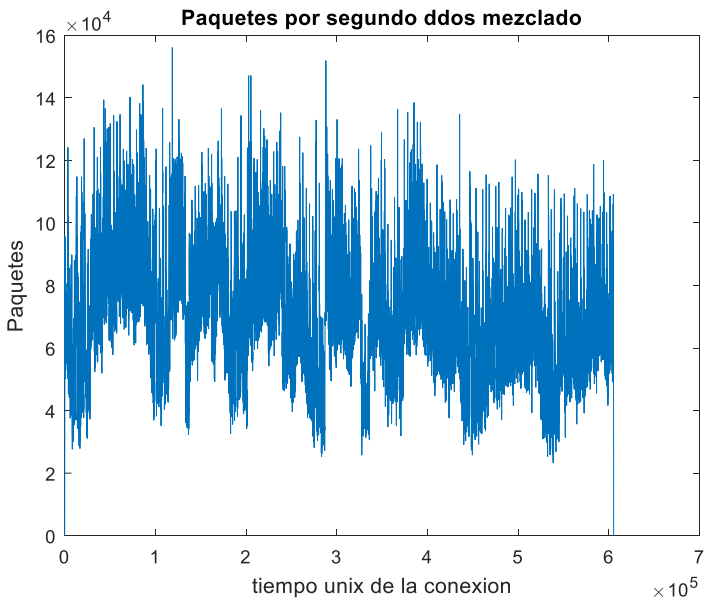


Ilustración 4.6 Tráfico mezclado en paquetes.

4.3.1.1.1 Análisis del ancho de banda basado en medidas estadísticas

Las gráficas que veremos a continuación pertenecen al tráfico real y mezclado ubicados en el punto del ataque de la ilustración 4.2. Se mostrará en la ilustración 4.5 la zona ampliada de estudio para la ventana de dos minutos, pero para la de 15 minutos no se va a mostrar, puesto que no presenta las suficientes muestras. Sin embargo, esto no resultará ningún impedimento en la conclusión del trabajo.

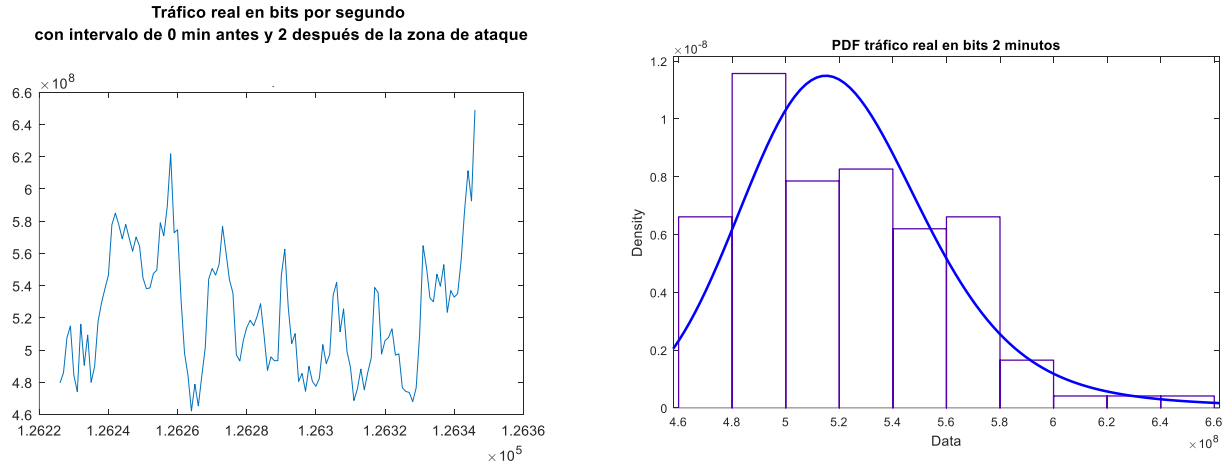


Ilustración 4.7 Tráfico real en bits de 2 minutos del ataque y su PDF.

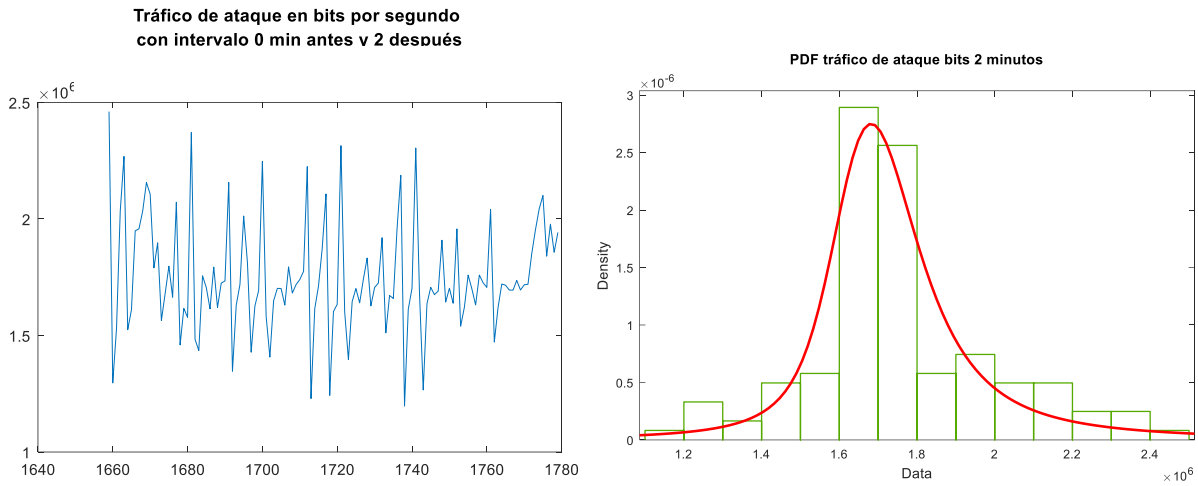


Ilustración 4.8 Tráfico de ataque en bits de 2 minutos del ataque y su PDF.

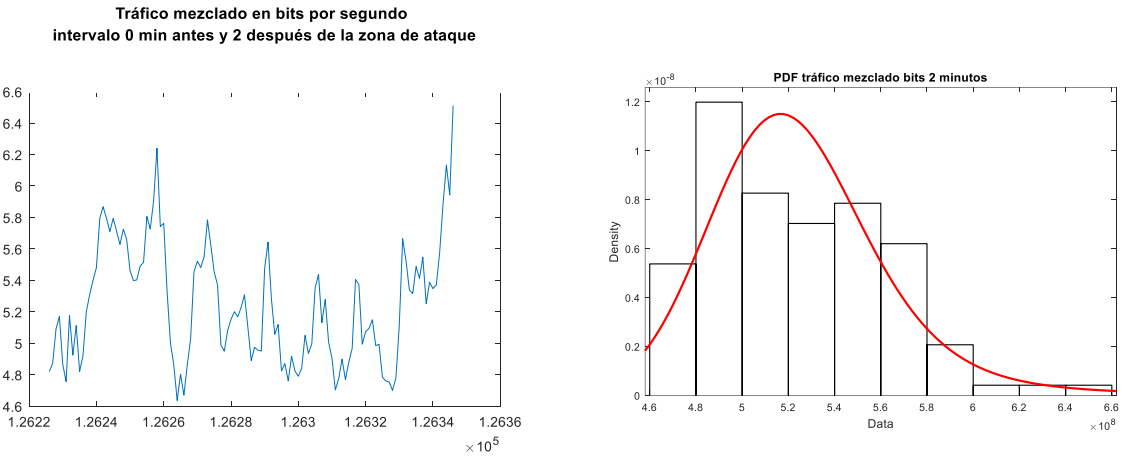


Ilustración 4.9 Tráfico mezclado en bits de 2 minutos del ataque y su PDF.

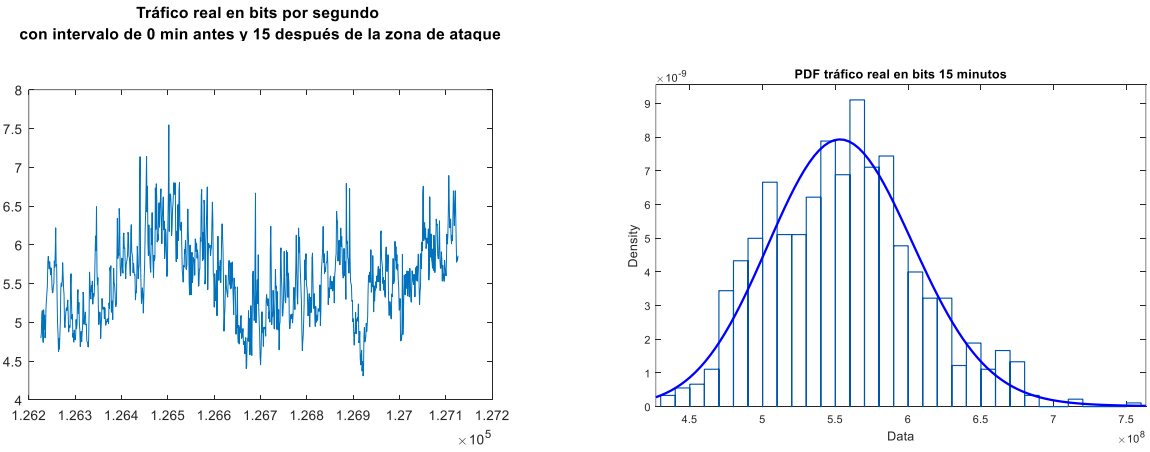


Ilustración 4.10 Tráfico real en bits de los 15 minutos del ataque y su PDF.

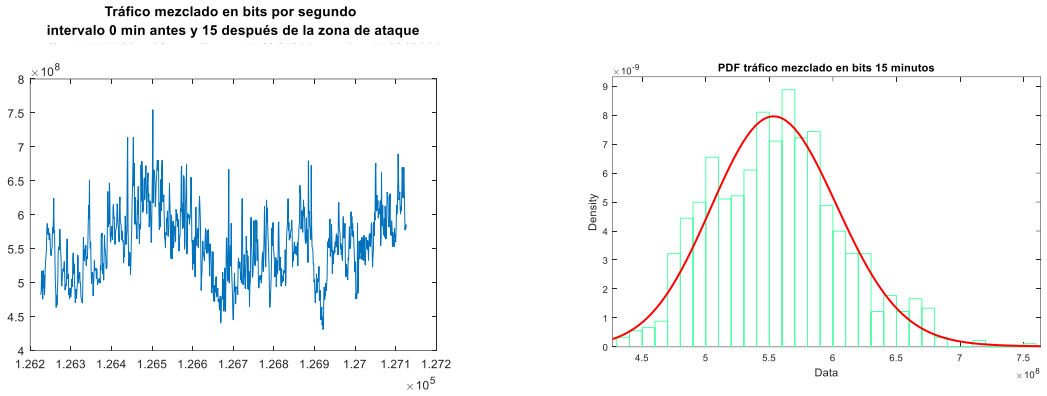


Ilustración 4.11 Tráfico mezclado en bits de los 15 min. del ataque y su PDF.

4.3.1.1.2 Análisis del ancho de banda basado en estimación de parámetros

Las ilustraciones que acabamos de ver corresponden a lo que se ha ido comentando a lo largo del trabajo. Para complementar estas ilustraciones y en la siguiente sección comentar los resultados, vamos a realizar el cálculo de los valores alfa-estable en cada una de las gráficas mostradas junto con la función de probabilidad de densidad (PDF) de cada una, estas se pueden observar en las anteriores ilustraciones. Como se ha mencionado antes para la de 15 minutos no tenemos muestras suficientes para la representación de la PDF, sin embargo, nos bastará con las representaciones de las ilustraciones.

	Real 2 minutos	Sintético 2 minutos	Mezclado 2 minutos	Real 15 minutos	Mezclado 15 minutos
α	1.99	1.34	1.99	1.99	1.99
β	1	0.36	1	1	1
γ	2.9 e+07	1.15e+05	2.92e+07	3.66e+07	3.63e+07
δ	5.16e+08	1.76e+06	5.17e+08	5.54e+08	5.54e+08

Tabla 4.1 Valores alfa estable del tráfico bits en los diferentes intervalos.

	Real 2 minutos	Sintético 2 minutos	Mezclado 2 minutos	Real 15 minutos	Mezclado 15 minutos
media	5.22e+08	1.74e+06	5.24e+08	5.55e+08	5.57e+08
mediana	5.16e+08	1.7e+06	5.17e+08	5.54e+08	5.54e+08
moda	4.62e+08	1.19e+06	4.63e+08	5.51e+08	5.51e+08
varianza	1.43e+15	5.78e+10	1.43e+15	2.63e+15	2.61e+15
Desviación típica	3.79e+07	2.40e+05	3.79e07	5.13e+07	5.11e+07

Tabla 4.2 Valores estadísticos del tráfico bits en los diferentes intervalos.

4.3.1.1.3 Análisis de la tasa de paquetes basado en medidas estadísticas

Una vez mostradas las gráficas de los bits por segundo y las tablas de sus parámetros alfa-estables falta representar lo mismo para los paquetes por segundo para, en la siguiente sección, comparar ambos casos. Respecto al cálculo de los parámetros alfa estable para los paquetes se procederá de la misma manera que para los bits.

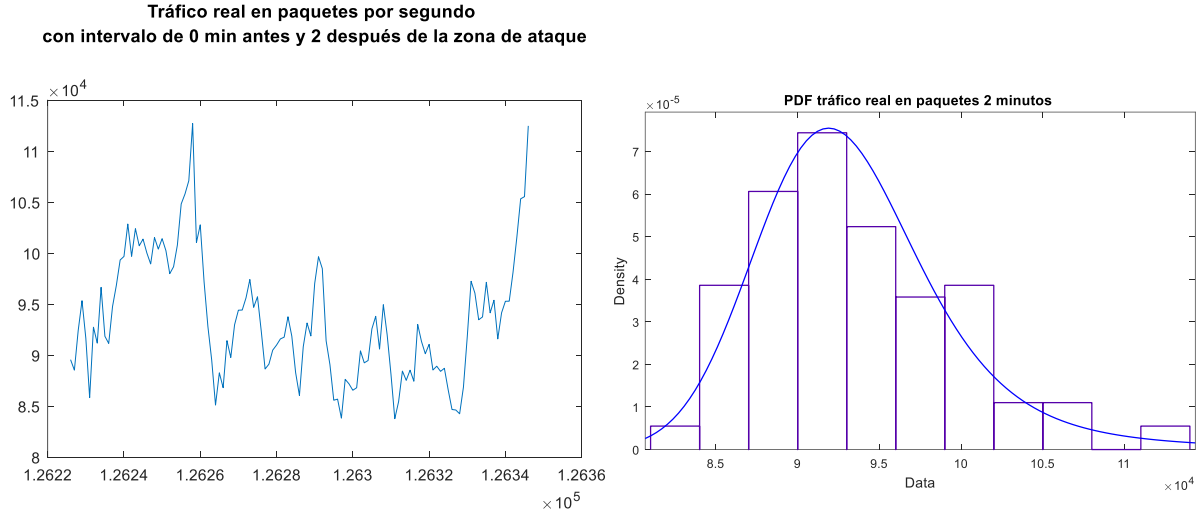


Ilustración 4.12 Tráfico real en paquetes de 2 minutos del ataque y PDF.

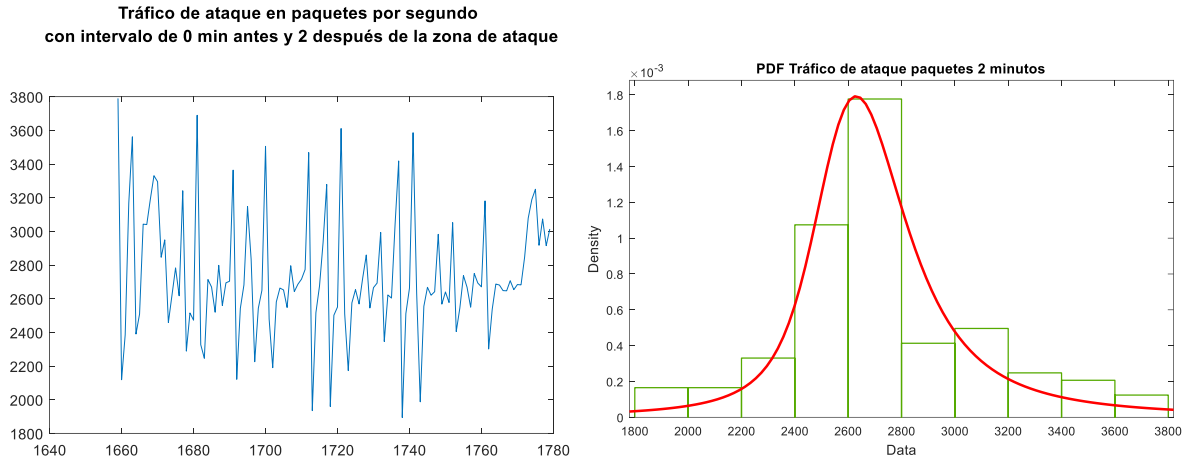


Ilustración 4.13 Tráfico ataque en paquetes de 2 minutos del ataque y su PDF.

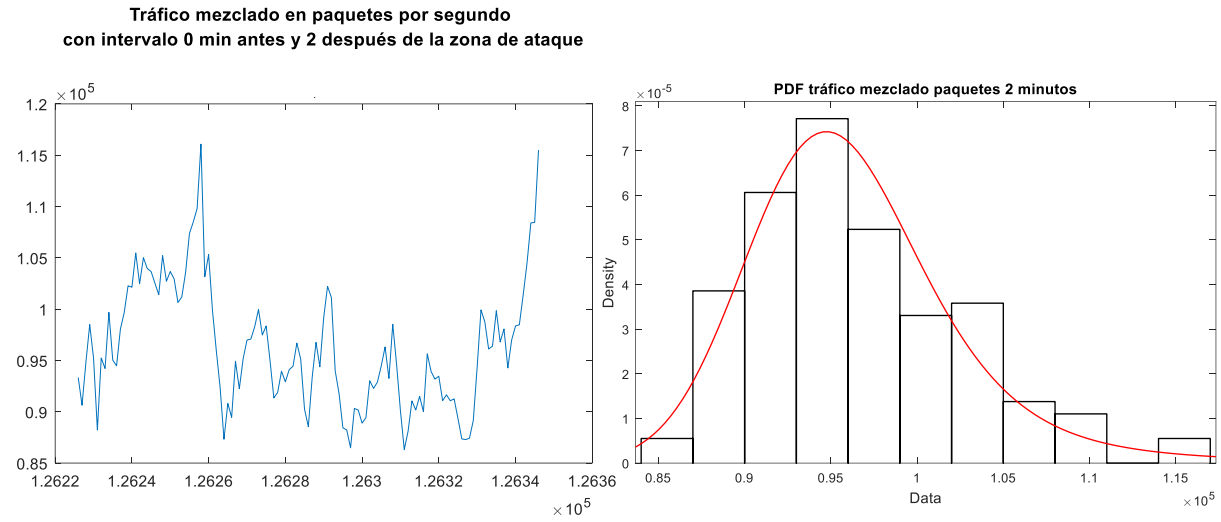


Ilustración 4.14 Tráfico mezclado en paquetes de 2 minutos del ataque y su PDF.

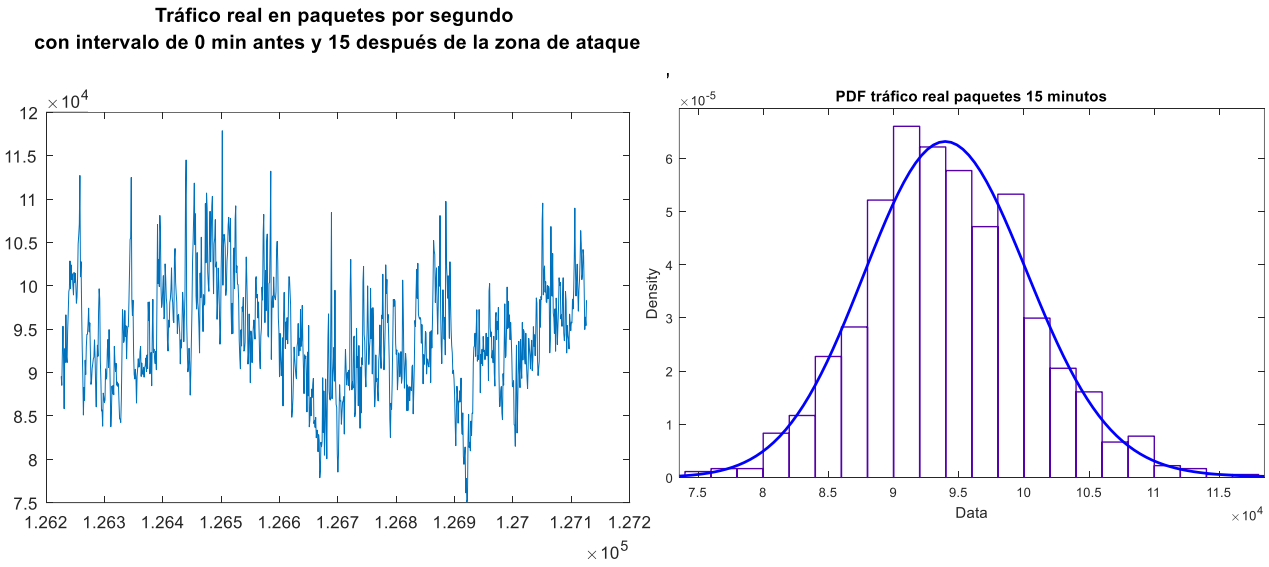


Ilustración 4.15 Tráfico real en paquetes de 15 minutos y su PDF.

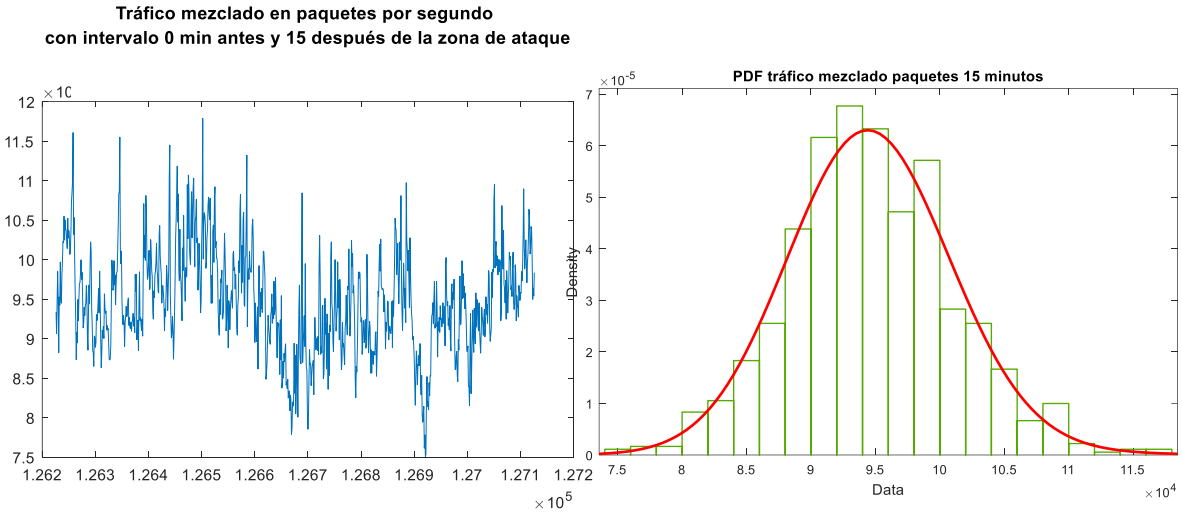


Ilustración 4.16 Tráfico mezclado en paquetes de 15 minutos y su PDF.

4.3.1.1.4 Análisis de la tasa de paquetes basado en estimación de parámetros

	Real 2 minutos	Sintético 2 minutos	Mezclado 2 minutos	Real 15 minutos	Mezclado 15 minutos
α	1.99	1.36	1.99	1.91	1.74
β	1	0.36	1	1	0.24
γ	4.35e+03	1.84e+02	4.30e+03	4.39e+03	4.09e+03
δ	9.24e+04	2.75e+03	9.51e+04	9.41e+04	9.46e+04

Tabla 4.3 Valores alfa estable del tráfico en paquetes en los diferentes intervalos.

	Real 2 minutos	Sintético 2 minutos	Mezclado 2 minutos	Real 15 minutos	Mezclado 15 minutos
media	9.35e+04	2.73e+03	9.63e+04	9.41e+04	9.46e+04
mediana	9.24e+04	2.66e+03	9.51e+04	9.38e+04	9.43e+04
moda	8.37e+04	1.89e+03	8.63e+04	9.09e+04	9.09e+04
varianza	3.64e+07	1.36e+05	3.71e+07	4.11e+07	4.14e+07
Desviación típica	6.03e+03	3.69e+02	6.09+03	6.41e+03	6.43e+03

Tabla 4.4 Valores estadísticos del tráfico paquetes en los diferentes intervalos.

Una vez se han mostrado los datos más característicos del ataque de denegación de servicio damos paso al otro tipo de ataque, que, en este caso, se trata de una serie de IPs malignas que se tenían en una lista negra.

4.3.2 Blacklist

En este apartado se va a realizar lo mismo que se ha hecho en la sección de denegación de servicio, vamos a mostrar la forma que tiene este tráfico, como es la mezcla del tráfico real y una zona de interés para observar el comportamiento de los estadísticos y los valores de

los parámetros alfa-estable. Hay que tener en cuenta que esto no se considera un ataque si no como spam que se recibe de servidores como Yahoo [5]

Igual que hemos realizado antes empezaremos mostrando los bits por segundo y después los paquetes por segundo para en la sección de resultados comentar las diferencias.

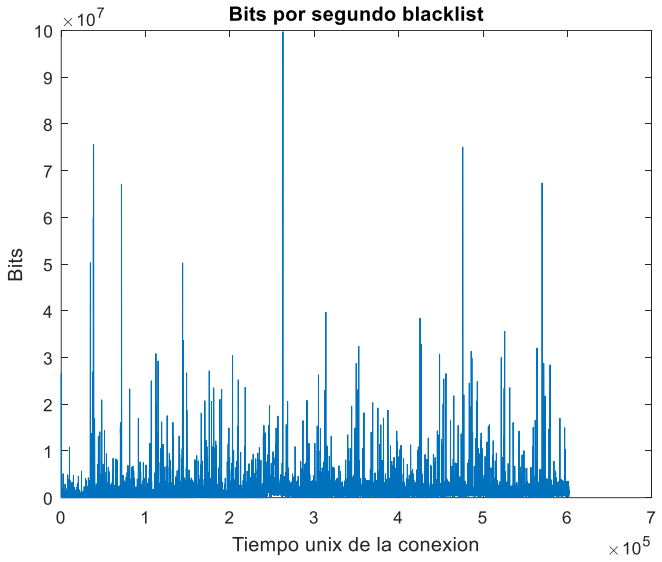


Ilustración 4.17 Tráfico de ataque blacklist en bits.

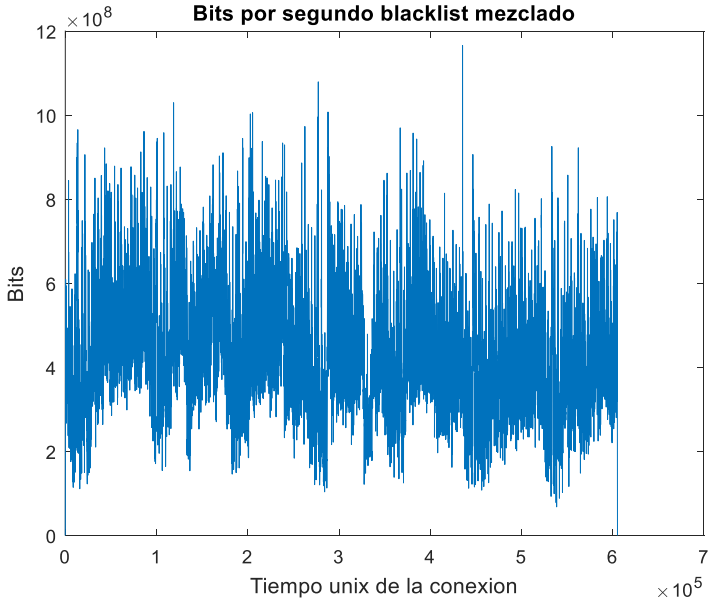


Ilustración 4.18 Tráfico mezclado en bits

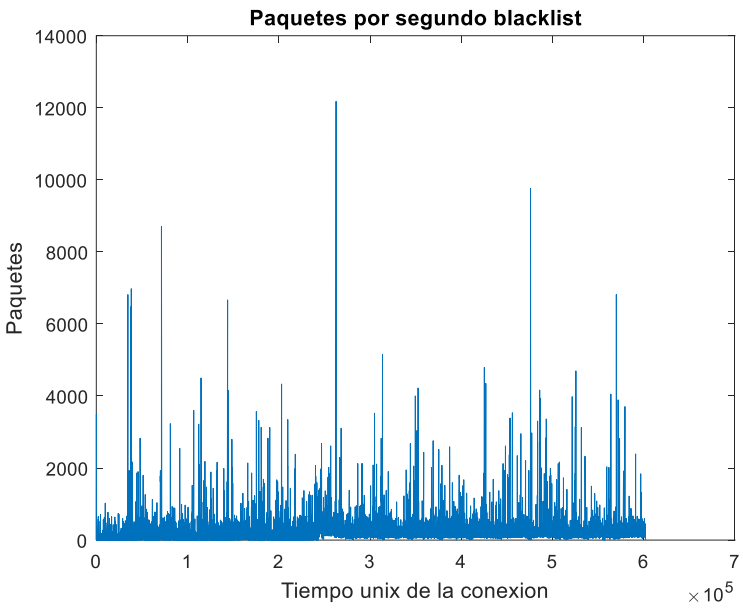


Ilustración 4.19 Tráfico de ataque blacklist en paquetes.

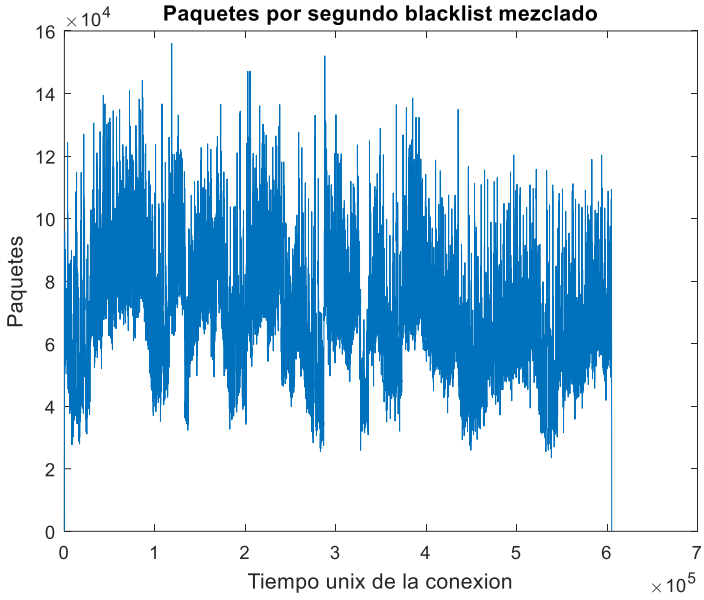


Ilustración 4.20 Tráfico mezclado en paquetes.

4.3.2.1.1 Análisis del ancho de banda basado en medidas estadísticas

En este tipo de anomalía, al no tener un pico igual de característico que en el caso anterior, nos vamos a centrar en el pico más grande que se encuentre y cogeremos los 15 minutos en adelante para ver sus características.

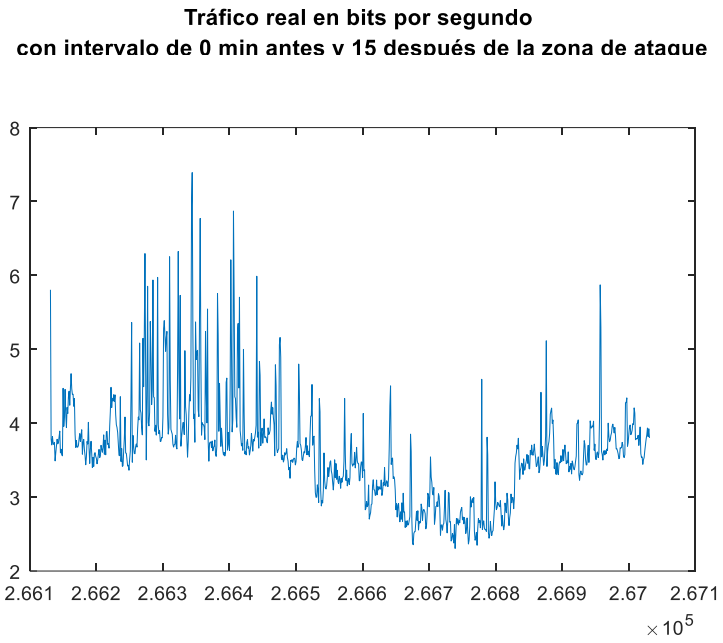


Ilustración 4.21 Tráfico real en bits de los 15 minutos del ataque.

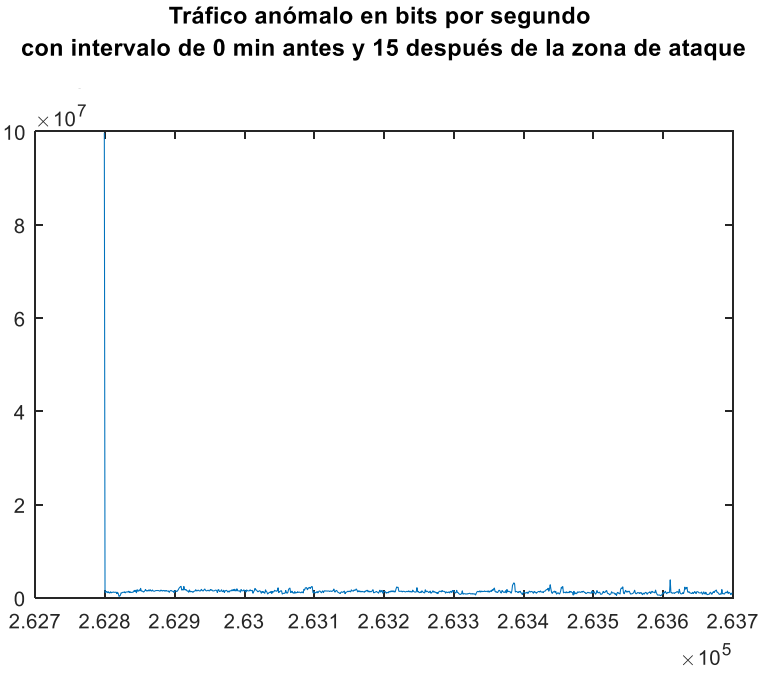


Ilustración 4.22 Tráfico de ataque en bits de los 15 minutos del ataque.

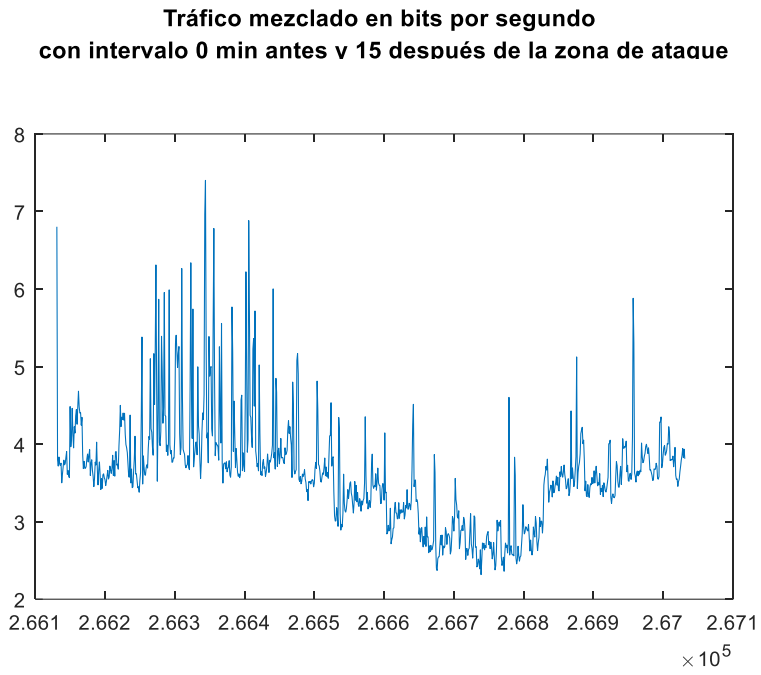


Ilustración 4.23 Tráfico mezclado en bits de los 15 minutos del ataque.

4.3.2.1.2 Análisis del ancho de banda basado en estimación de parámetros

Puesto que la representación en paquetes es muy parecida, pero con valores menores en el eje Y, adjuntaremos las representaciones en el Anexo A, junto con las tablas de cada una de ellas, como las que veremos a continuación, pero para los paquetes.

	Real 15 minutos	Sintético 15 minutos	Mezclado 15 minutos
α	1.34	1.65	1.34
β	0.26	0.50	0.26
γ	3.18e+07	1.96e+05	3.18e+07
δ	3.70e+08	1.31e+06	3.71e+08

Tabla 4.5 Valores alfa estable del tráfico en bits en 15 minutos.

	Real 15 minutos	Sintético 15 minutos	Mezclado 15 minutos
media	3.60e+08	1.41e+06	9.63e+04
mediana	3.59e+08	1.27e+06	9.51e+04
moda	2.50+e08	1.07e+6	8.63e+04
varianza	4.81e+15	1.08e+13	3.71e+07
Desviación típica	6.94+e07	3.29e+06	6.09+03

Tabla 4.6 Valores estadísticos del tráfico en bits en 15 minutos.

Con estos valores acabamos de mostrar los valores más característicos de ambos ataques, en el trabajo se le ha dado más importancia a la denegación de servicio por ser un ataque directo a la red, no como en el caso de las listas negras de IPs que se tratan de direcciones bloqueadas por spam.

4.4 Resultados

En el apartado anterior se han mostrado las características más importantes de ambos ataques para que en esta sección se comparen dichos valores y ver que tienen en común.

Primero empezaremos con el ataque de denegación de servicio.

- Si observamos el comportamiento de los estadísticos parecen exactamente iguales tanto para bits como para paquetes. A la vista de esto, se añade el comportamiento de los valores como la media y mediana en las zonas de estudio para poder apreciar ciertas diferencias. Además, también están los parámetros alfa-estable con los cuales vamos a ver con cuál parece que se detecta más la anomalía. Para poder visualizar mejor la diferencia se marca en la tabla 4-14 y 4-15 las diferencias en porcentaje de la media y del valor de la alfa, puesto que como se explica en el capítulo 2, marca la forma de la curva. Estas diferencias son calculadas para los dos minutos y para los 15 minutos, comparando el tráfico real y el mezclado, por este motivo se decía anteriormente que los valores entre medias de estos valores no impedían llegar a la conclusión del trabajo.

	2 minutos	15 minutos
$\Delta\bar{x}$	0.33%	0.04%
$\Delta\alpha$	0%	0%

Tabla 4.7 Diferencia en porcentaje de los datos en bits.

	2 minutos	15 minutos
$\Delta\bar{x}$	2.91%	0.45%
$\Delta\alpha$	0%	8.72%

Tabla 4.8 Diferencia en porcentaje de los datos en paquetes.

- Con estos valores que acabamos de ver podemos decir que la mejor forma de ver cuánto ha variado el estadístico es con los paquetes por segundo y no con los bits. Además, con la variable alfa es con la que se ha detectado mayor diferencia, por tanto, lo que se va a hacer es realizar el mismo análisis del tráfico real y el mezclado de los paquetes en un plazo de dos horas con una ventana de 15 minutos calculando los valores de alfa estable. En la ilustración 4.24 se observa dos valores de alfa, el color azul representa el tráfico original y el rojo el mezclado. El valor de alfa a lo largo de 4 horas, siendo dos horas antes del ataque y otras dos después, se mantiene igual para el normal y el mezclado, pero cuando llega a la zona del ataque es cuando esos valores se separan. Esa separación indica que gracias a los valores del alfa en ese punto se está produciendo una anomalía en la red.

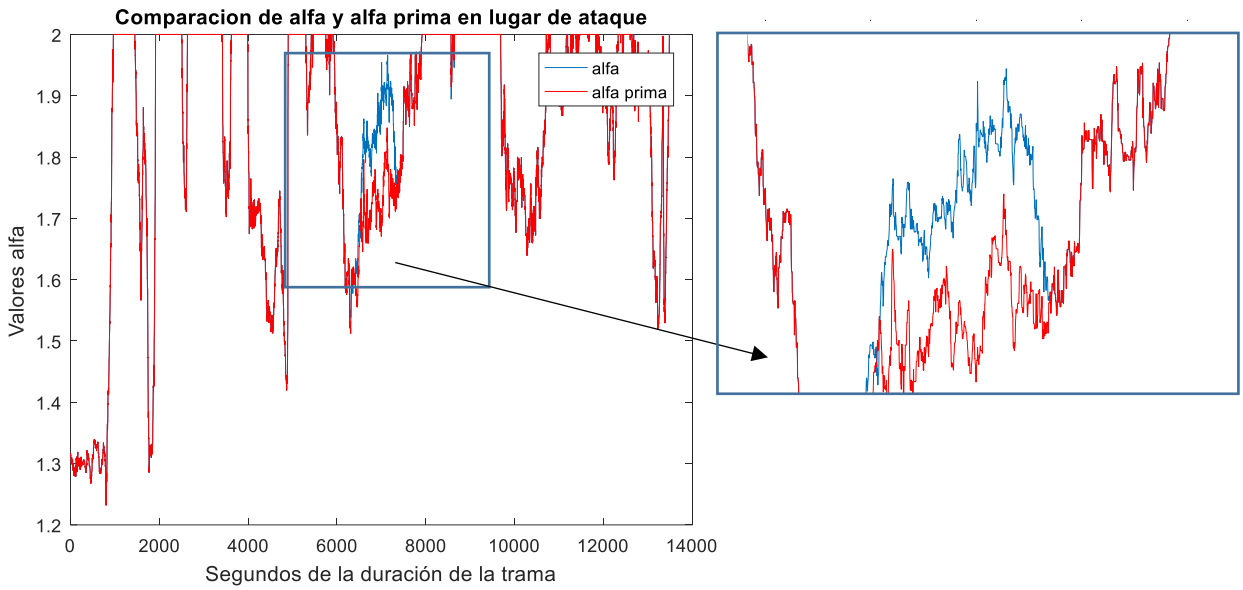


Ilustración 4.24 Representación de alfa a lo largo de 4 horas con ventana de 15 minutos.

- Los otros valores como la beta, gamma y delta sufren variaciones, pero no tan significativos como la alfa, por lo que vienen en el Anexo A.

Si ahora analizamos el comportamiento que sigue la anomalía de blacklist nos encontramos con:

- En las gráficas observamos lo mismo que en el caso de la denegación de servicio, en el cual son casi idénticas. Debido a esto, debemos mirar los valores de la media y de los parámetros alfa como hemos hecho anteriormente para ver con cuál de las medidas es mejor. En las dos siguientes tablas podemos observar esto.

	2 minutos	15 minutos
$\Delta\bar{x}$	0.58%	0.39%
$\Delta\alpha$	0.94%	0.00%

Tabla 4.9 Diferencia en porcentaje de los datos blacklist en bits..

	2 minutos	15 minutos
$\Delta\bar{x}$	0.64%	0.50%
$\Delta\alpha$	0%	0.41%

Tabla 4.10 Diferencia en porcentaje de los datos blacklist en paquetes.

- En este caso, la detección con los parámetros alfa-estable no parece la más acertada, sin embargo, vamos realizar el mismo análisis que en el caso anterior para ver como varían estos parámetros a lo largo del tiempo.

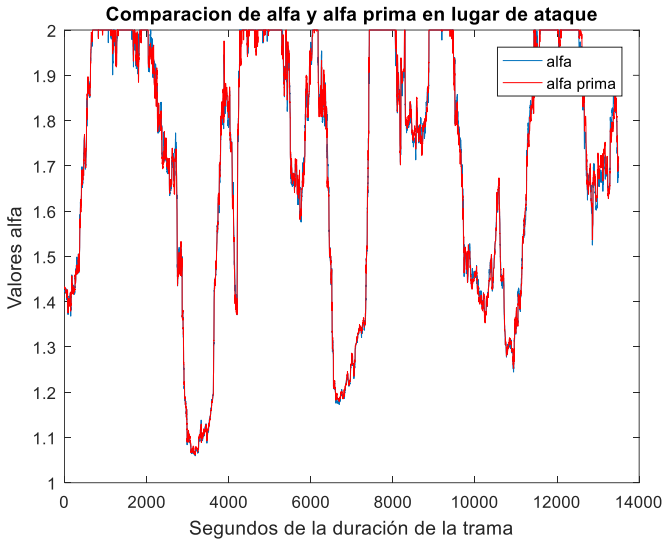


Ilustración 4.25 Representación de alfa a lo largo de 4 horas con ventana de 15 minutos.

- Tal y como habíamos predicho el análisis de los valores alfa-estable en este caso no nos aporta donde se produce el ataque. Las representaciones de los demás valores se encuentran en el Anexo A.

4.5 Conclusiones

En esta sección se van a relacionar todos los conceptos que hemos visto en este apartado para en el siguiente capítulo, acabar de aclararlos y proponer los posibles trabajos futuros.

Como hemos visto, los ataques pueden no ser detectados a simple vista con solo analizando la forma que presentan los datos por segundo. Además, los cálculos de media, moda, mediana, etc tampoco aportan claridad sobre si está ocurriendo algo en la red, sufren una pequeña variación, pero nada notorio. Sin embargo, los parámetros del modelo alfa-estable han supuesto una gran ventaja frente a éstos puesto que su variación sí que ha permitido detectar en uno de los casos la amenaza.

Por otra parte, si observamos las PDF que hay en el apartado anterior llegamos a una conclusión muy interesante. El efecto que se va a comentar se observa mucho mejor con las PDF correspondientes a los 2 minutos del análisis para los paquetes por segundo. El proceso de mezclar el tráfico real con el de ataque sintético se puede ver como la convolución de las

funciones de probabilidad de densidad de estas dos que dan lugar a la de la PDF del tráfico mezclado puesto que tanto el número de paquetes y bits por segundo son una variable aleatoria, la suma de estas dos da como resultado otra variable aleatoria. Esto es debido a que la PDF del tráfico de ataque se puede modelar como una delta en un punto que desplaza la PDF del tráfico real a donde se ubica la mezclada. Sin embargo, para los 15 minutos el efecto que se observa es que el desplazamiento que se produce es tan pequeño que apenas se ve desplazado pero la forma de la PDF si se ve alterada, con esto se demuestra que el ataque se puede detectar a través del parámetro alfa. De manera que el proceso es el siguiente:

PDF de los datos procesados en dos minutos.

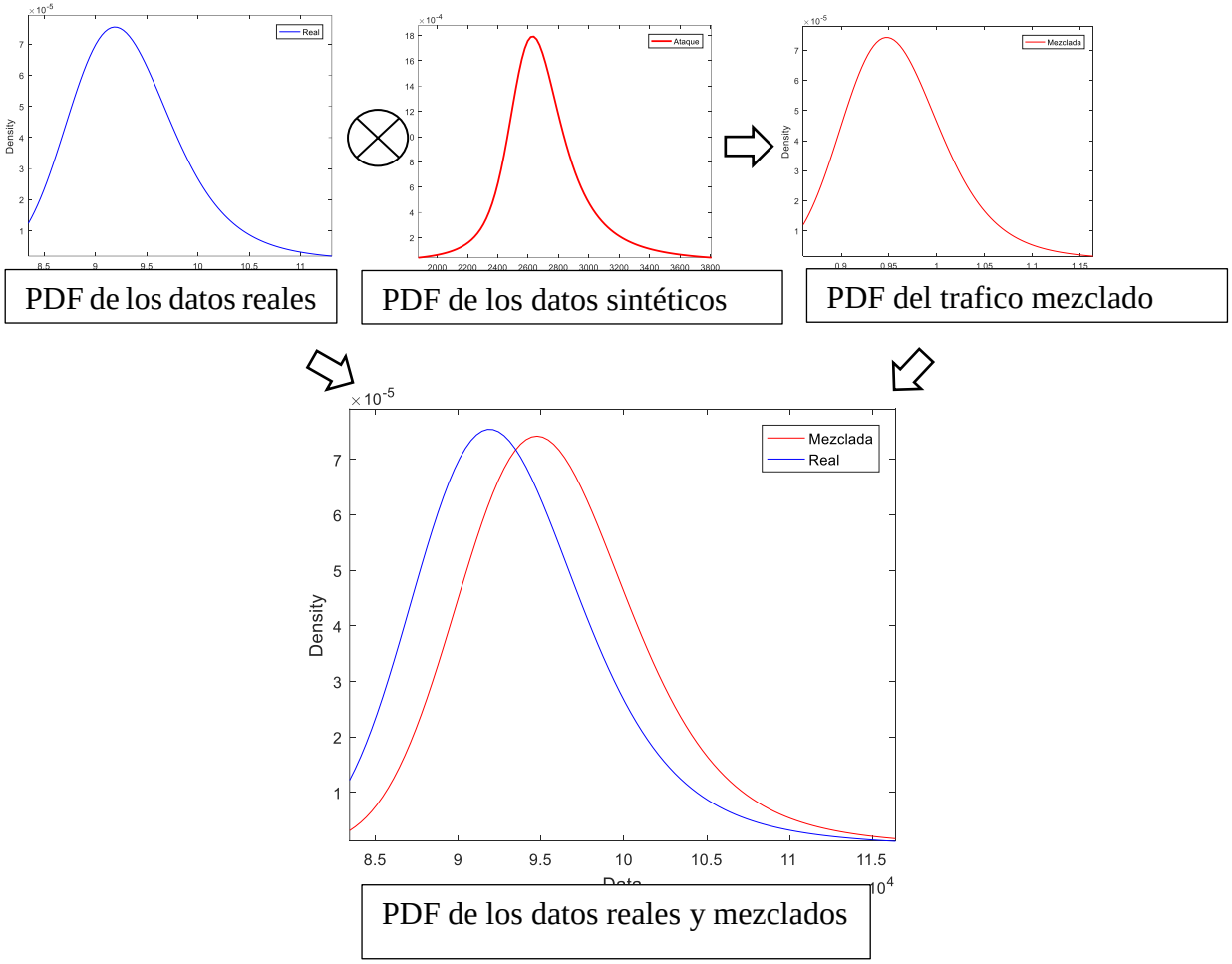


Ilustración 4.26 Demostración de la convolución en dos minutos.

PDF de los datos procesados en quince minutos.

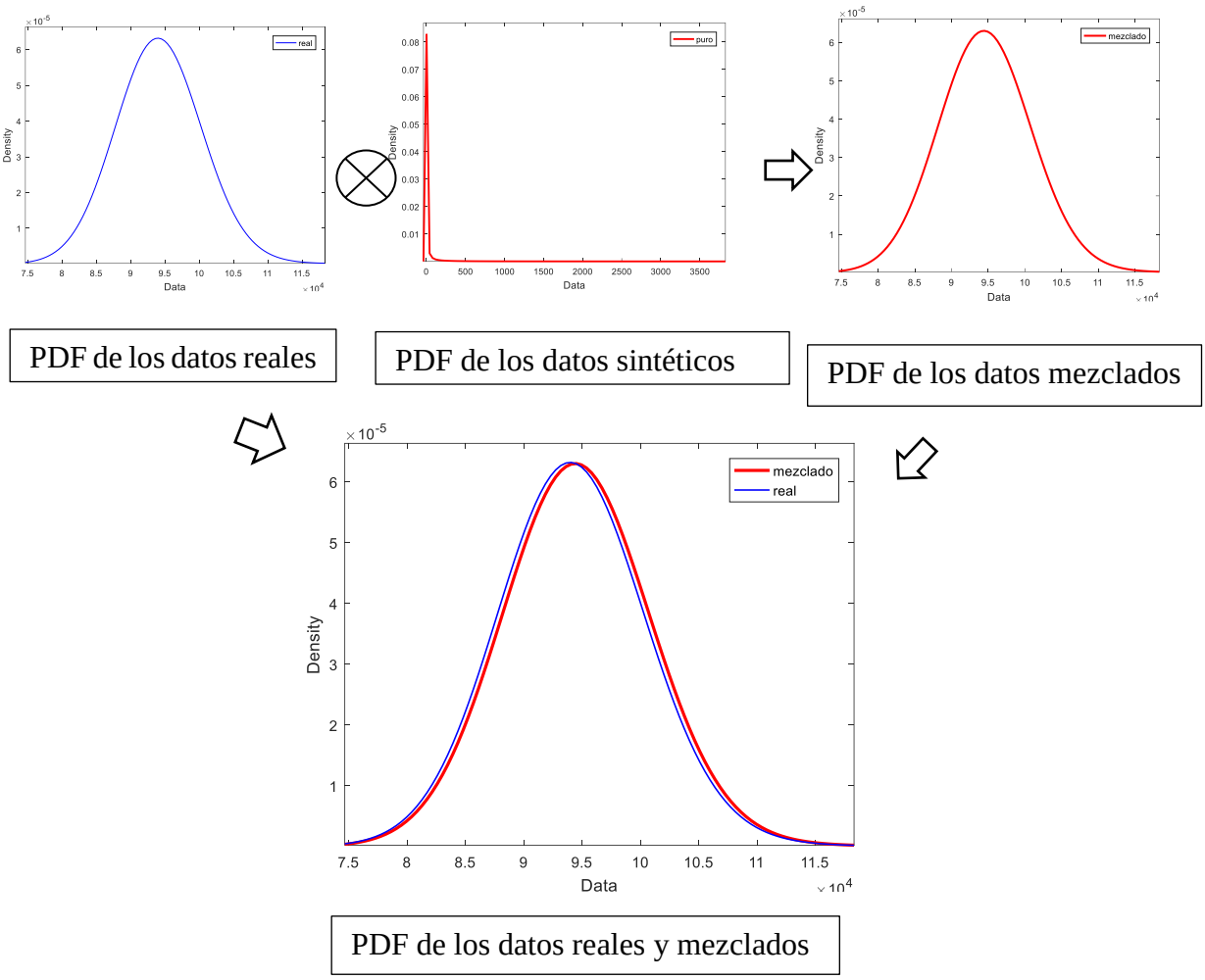


Ilustración 4.27 Demostración de la convolución en quince minutos.

5.Conclusiones y trabajo futuro

5.1 Conclusiones

En este apartado se van a desarrollar las conclusiones de todo el trabajo que se ha ido creando para poder realizar el análisis.

Hemos partido de una serie de archivos de los cuales hemos extraído su información y la hemos analizado para saber la forma que tenían. De este primer análisis, nos dimos cuenta de que las tramas de redes se podían mezclar para generar unas tramas que hemos llamado tráfico mezclado. Este tráfico nos ha sido muy útil para ver cómo se comportan los dos tipos de ataques/anomalías que hemos usado. Además, con este mismo tráfico se han probado valores estadísticos típicos para ver como variaban respecto del tráfico real. Al ver que estos valores no nos resultaban muy útiles o no presentaban los cambios que esperamos se le ha aplicado un modelo estadístico denominado alfa-estable, con el cual hemos podido ver en uno de los casos el comportamiento que tenía. Por último, tras ver estos datos variar, nos hemos dado cuenta de una última reflexión con la cual hemos cerrado el capítulo anterior. Esta es que la PDF del tráfico de ataque convolucionada con la PDF del tráfico real genera la PDF del tráfico mezclado. Además, para cada periodo de análisis se observa una cualidad distinta: para el de dos minutos destaca que con la media podemos detectar que se produce una anomalía, mientras que, con el análisis en quince minutos, la detección con la media no es posible y solo se detectará la anomalía con la variación de la curva que se produce en el resultado de la convolución, es decir, la variable α de los parámetros alfa-estable.

5.2 Trabajo futuro

De cara a trabajos futuros, se podrían hacer las siguientes cosas:

- Determinar la veracidad de lo expuesto realizando más pruebas en diferentes entornos y diferentes datos.
- Implementar un sistema que intente predecir el valor que tendrá el alfa estable de esta manera poder determinar que puede ocurrir en la red.

- Determinar cuál es el factor que hace que los parámetros alfa estable se vean modificados pero los valores estadísticos típicos no.
- Si se consigue determinar un sistema que prediga de manera correcta el valor del alfa-estable que a su vez se determine que valores son considerados buenos y cuales nocivos para la red.

Referencias

[1] Prevención de intrusiones. Ayuda de Kaspersky Internet Security. https://help.kaspersky.com/KIS4Mac/16.0/es.lproj/pgs/88075.htm

[2] Álvaro Gómez Vieites "Tipos de ataques e intrusos en las redes informáticas"

[3] Jaime Blasco Bermejo "Ataques DoS en aplicaciones Web"

[4] J. L. García-Dorado, J. E. López, J. Aracil, V. López, J. A. Hernández, S. López-Buedo y L. de Pedro. "Utilidad de los flujos NetFlow de RedIRIS para análisis de una red académica"

[5] Gabriel Maciá Fernández, José Camacho, Roberto Magán-Carrión, Marta Fuentes-García, Pedro García-Teodoro. "UGR' 16:Un nuevo conjunto de datos para la evaluación de IDS de red"

[6] Jhon P. Nolan. "Stable Distributions"

[7] Federico Jesús Simmross Wattenberg. "Detección de anomalías en el tráfico agregado de redes IP basada en inferencia estadística sobre un modelo α-estable de primer orden"

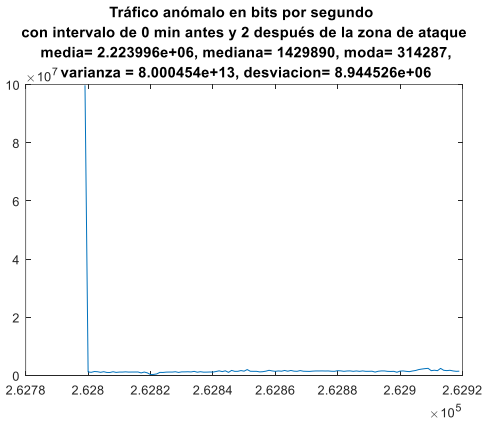
[8] Ejemplo de distribución alfa estable.

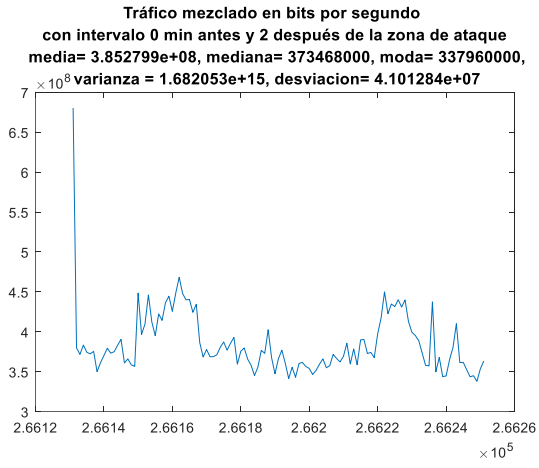
https://commons.wikimedia.org/wiki/File:Levy_distributionPDF.pn

Anexos

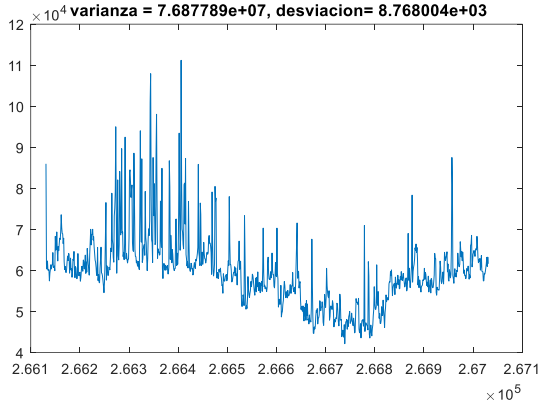
A Gráficas adicionales

A continuación, se muestras las gráficas que se han ido realizando a lo largo del trabajo. Es importante destacar que no son gráficas que no tengan valor, si no que debido a la cantidad de estas se ha decidido que dentro de las importantes estas pasaran a un segundo plano y sean usadas como apoyo.

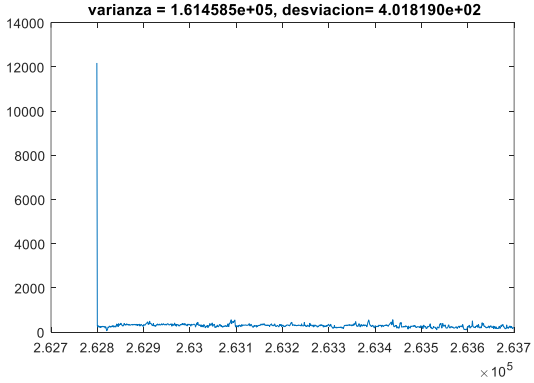




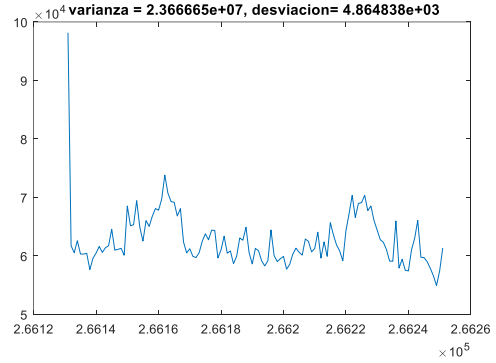
Tráfico real en paquetes por segundo
con intervalo de 0 min antes y 15 después de la zona de ataque
media= 5.981586e+04, mediana= 5.937740e+04, moda= 4.214470e+04,
varianza = 7.687789e+07, desviacion= 8.768004e+03



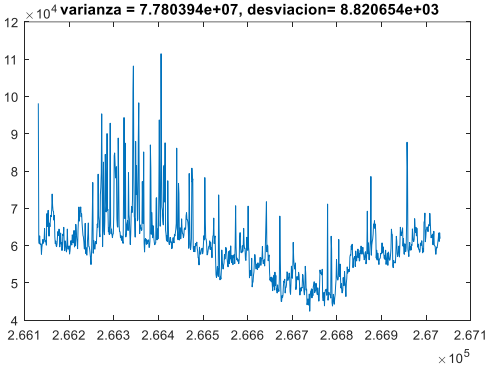
Tráfico anómalo en paquetes por segundo
con intervalo de 0 min antes y 15 después de la zona de ataque
media= 2.994071e+02, mediana= 2.876180e+02, moda= 2.969660e+02,
varianza = 1.614585e+05, desviacion= 4.018190e+02



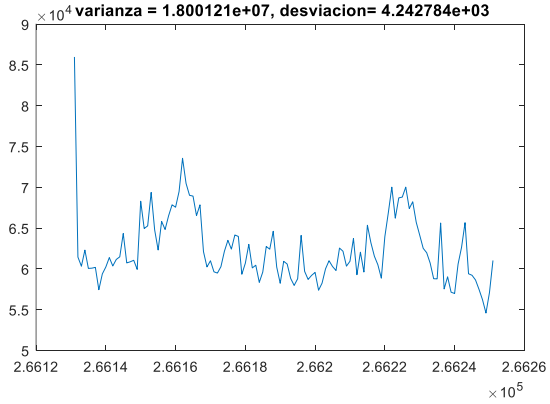
Tráfico mezclado en paquetes por segundo
con intervalo 0 min antes y 2 después de la zona de ataque
media= 6.277672e+04, mediana= 6.131740e+04, moda= 5.491940e+04,
varianza = 2.366665e+07, desviacion= 4.864838e+03



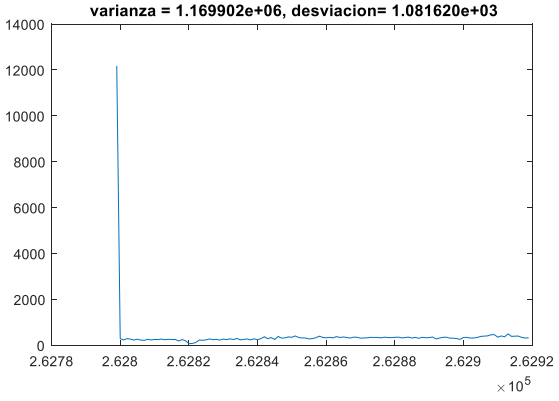
Tráfico mezclado en paquetes por segundo
con intervalo 0 min antes y 15 después de la zona de ataque
media= 6.011527e+04, mediana= 5.970460e+04, moda= 5.638170e+04,
varianza = 7.780394e+07, desviacion= 8.820654e+03



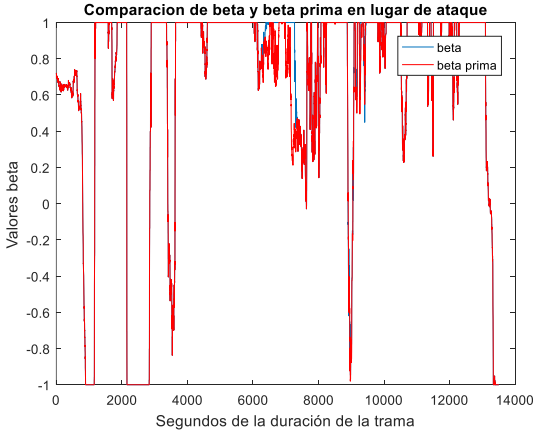
Tráfico real en paquetes por segundo
con intervalo de 0 min antes y 2 después de la zona de ataque
media= 6.237559e+04, mediana= 6.102820e+04, moda= 5.458190e+04,
varianza = 1.800121e+07, desviacion= 4.242784e+03



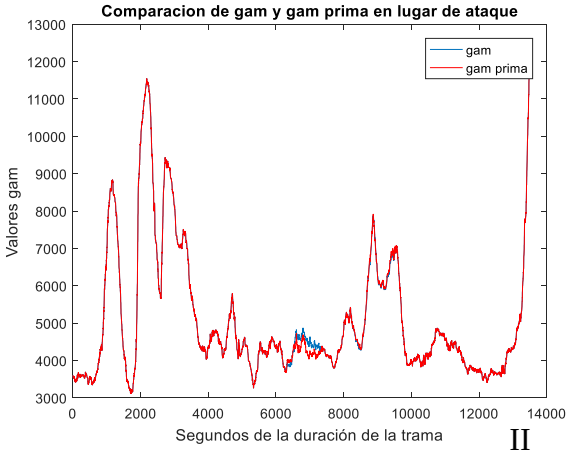
Tráfico anómalo en paquetes por segundo
con intervalo de 0 min antes y 2 después de la zona de ataque
media= 4.011192e+02, mediana= 3.133480e+02, moda= 3.188370e+02,
varianza = 1.169902e+06, desviacion= 1.081620e+03

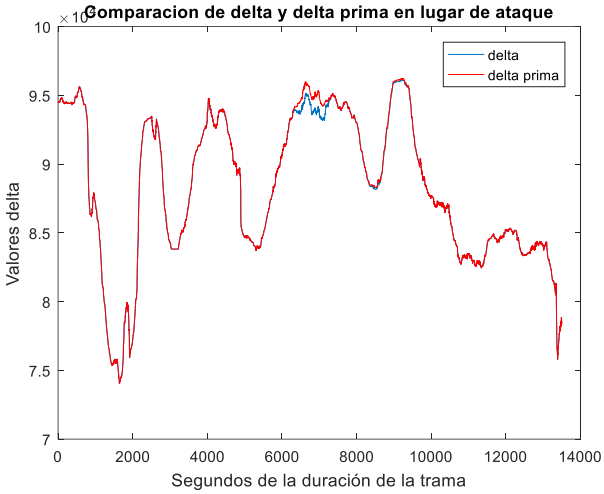


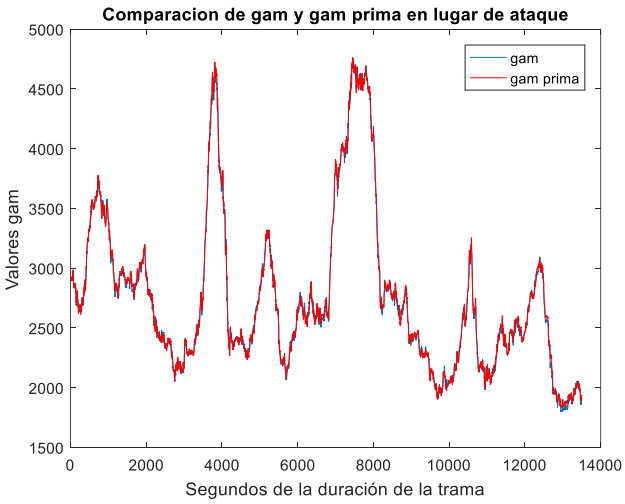
Comparacion de beta y beta prima en lugar de ataque

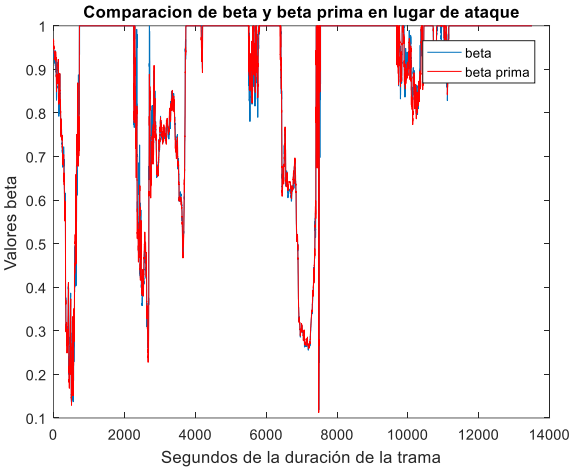


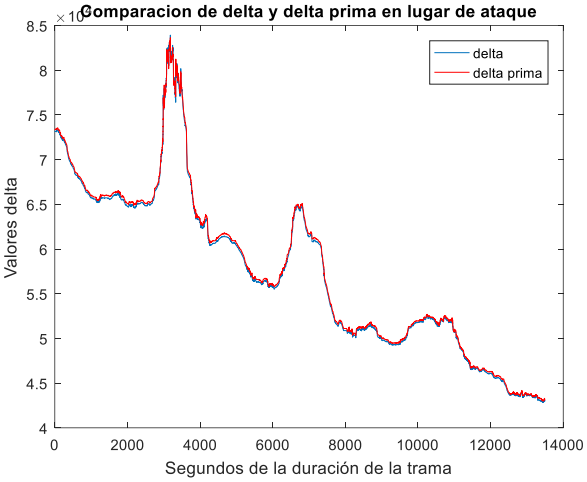
Comparacion de gam y gam prima en lugar de ataque




Comparacion de delta y delta prima en lugar de ataque
×10^4
delta
delta prima
Valores delta
Segundos de la duración de la trama


Comparacion de gam y gam prima en lugar de ataque
gam
gam prima
Valores gam
Segundos de la duración de la trama


Comparacion de beta y beta prima en lugar de ataque
beta
beta prima
Valores beta
Segundos de la duración de la trama


Comparacion de delta y delta prima en lugar de ataque
×10^4
delta
delta prima
Valores delta
Segundos de la duración de la trama

B Tablas adicionales

Como se ha comentado al principio del anexo A, en este anexo ocurre lo mismo, las tablas que se muestran son importantes porque entran dentro de la comparativa que se realiza.

	Real 2 minutos	Sintético 2 minutos	Mezclado 2 minutos
α	1.73	1.69	1.74
β	1	0.98	1
γ	1.89e+07	1.78e+05	1.89e+07
δ	3.77e+08	1.48e+06	3.78e+08

Tabla B-1. Valores alfa estable del tráfico real en bits de blacklist

	Real 2 minutos	Sintético 2 minutos	Mezclado 2 minutos
α	1.99	1.99	1.99
β	1	-1	1
γ	2.61e+03	44.42	2.57e+03
δ	6.10e+04	3.13e+02	6.13e+04

Tabla B-2. Valores alfa estable del tráfico real en paquetes de blacklist

	Real 15 minutos	Sintético 15 minutos	Mezclado 15 minutos
α	1.34	1.87	1.33
β	0.26	0.05	1
γ	3.99e+03	42.96	3.97e+03
δ	6.11e+04	2.87e+02	6.11e+04

Tabla B-2. Valores alfa estable del tráfico real en paquetes de blacklist